



Networking the world's business data™

# INTREPID DIRECTOR 6140

## Intrepid® 6140 Director Installation and Service Manual

P/N 620-000157-410  
REV A

### Simplifying Storage Network Management

McDATA Corporation  
380 Interlocken Crescent Broomfield, CO 80021-3464  
Corporate Headquarters: 800-545-5773  
Sales E-mail: [sales@mcdata.com](mailto:sales@mcdata.com) Web: [www.mcdata.com](http://www.mcdata.com)



## Record of Revisions and Updates

Revision	Date	Description
620-000157-000	9/2002	Initial release of the manual
620-000157-100	10/2002	Updates to describe Release 6.2 and 6.3 of the Enterprise Fabric Connectivity Manager application.
620-000157-200	2/2003	Updates to describe Release 7.1 of the Enterprise Fabric Connectivity Manager application. New cover and new format.
620-000157-201	6/2003	Updates to describe new firmware and software download procedures from McDATA's home page.
620-000157-300	8/2003	Revision of the manual to describe the one unit (1U) rack-mount server and Release 7.2 of the Enterprise Fabric Connectivity Manager application.
620-000157-400	12/2003	Revision of the manual to describe Release 8.0/8.1 of the Enterprise Fabric Connectivity Manager application. New style for safety notices. Addition of translated safety notices.
620-000157-410	1/2005	Revision of the manual to describe Release 8.5 of the Enterprise Fabric Connectivity Manager application, and the 10 Gbps (XPM) port card and functionality. Also includes update to EOS 7.0.

---

**Copyright © 2002 - 2005 McDATA Corporation. All rights reserved.**

Printed January 2005  
Sixth Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without prior written consent of McDATA Corporation.

The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer software programs described in this document. McDATA Corporation retains all rights, title and interest in the computer software programs.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.





<b>Preface .....</b>	<b>xxiii</b>
----------------------	--------------

## **Chapter 1      General Information**

Director Description .....	1-1
Field-Replaceable Units .....	1-4
Power/System LED Assembly .....	1-5
CTP Card.....	1-5
UPM Card .....	1-7
XPM Card .....	1-8
SFP and XFP Transceivers .....	1-9
Power Supply .....	1-10
AC Module .....	1-11
Fan Module.....	1-11
SBAR Assembly .....	1-11
Backplane .....	1-12
Error-Detection, Reporting, and Serviceability Features .....	1-12
Element Manager Status Indicators .....	1-14
Tools and Test Equipment.....	1-15
Tools Supplied with the Director.....	1-15
Tools Supplied by Service Personnel .....	1-17
Director Management .....	1-18

## **Chapter 2      Installation Tasks**

Factory Defaults .....	2-1
Installation Options .....	2-3
Summary of Installation Tasks.....	2-3
Task 1: Verify Installation Requirements .....	2-8
Task 2: Install the Ethernet Hub.....	2-9

Task 3: Install the Director .....	2-12
Subtask A: Unpack and Inspect the Director .....	2-12
Subtask B: Rack-Mount Installation.....	2-13
Subtask C: Turn-on Director Power.....	2-13
Task 4: Configure Director Network Information.....	2-15
Subtask A: Set Network Addresses (IP Address, Subnet mask, Gateway Address).....	2-15
Subtask B: LAN-Connect the Director.....	2-19
Task 5: Install the Management Server .....	2-20
Task 6: Configure the Management Server .....	2-22
Subtask A: Configure Password and Network Addresses.....	2-22
Subtask B: Configure Management Server Information....	2-25
Subtask C: Configure Windows 2000 Users .....	2-30
Subtask D: Set Management Server Date and Time .....	2-36
Subtask E: Configure the Call-Home Feature .....	2-38
Subtask F: Record or Verify Management Server Restore In- formation .....	2-39
Task 7: Configure Director to the SAN Management Application. 2-39	
Subtask A: Assign User Names and Passwords to SAN Man- agement Application.....	2-39
Subtask B: Identify the Director to the SAN Management Ap- plication .....	2-42
Subtask C: Verify Director-to-SAN Management Application Communication .....	2-43
Subtask D: Configure Feature Key.....	2-45
Subtask E: Configure Open Systems Management Server (OSMS) or FICON Management Server (FMS) .....	2-46
Configure OSMS.....	2-46
Configure FMS (FICON) .....	2-47
Task 8: Configure the Director at the Element Manager Application .....	2-49
Subtask A: Set Director Date and Time .....	2-50
Subtask B: Configure Director Identification .....	2-51
Subtask C: Configure Director Management Style.....	2-52
Subtask D: Configure Director Parameters .....	2-53
Subtask E: Configure Fabric Parameters.....	2-55
Subtask F: Configure Preferred Paths .....	2-57
Subtask G: Configure Switch Binding.....	2-59
Subtask H: Configure Director Ports .....	2-63
Subtask I: Configure SNMP Trap Message Recipients .....	2-66
Subtask J: Configure Threshold Alerts.....	2-67
Subtask K: Configure OpenTrunking.....	2-71

Subtask L: Enable SANpilot Interface and Telnet Access .....	2-73
Subtask M: Configure, Enable, and Test E-mail Notification... 2-73	
Subtask N: Configure and Enable Ethernet Events .....	2-75
Subtask O: Configure, Enable, and Test Call-Home Notifica- tion .....	2-76
Task 9: Configure SANtegrity Authentication (Optional).....	2-77
Accessing SANtegrity Authentication .....	2-77
Task 10: Back Up Configuration Data .....	2-78
Task 11: Configure the Director at the SANpilot Interface.....	2-80
Subtask A: Connect Director to Internet or Ethernet LAN Segment .....	2-82
Subtask B: Open the SANpilot Interface .....	2-82
Subtask C: Configure Director Ports .....	2-84
Subtask D: Configure BB Credit .....	2-85
Subtask E: Configure Director Identification.....	2-86
Subtask F: Configure Date and Time .....	2-87
Subtask G: Configure Operating Parameters .....	2-88
Subtask H: Configure Fabric Parameters .....	2-91
Subtask I: Configure Network Information .....	2-93
Subtask J: Configure SNMP .....	2-95
Subtask K: Enable or Disable the CLI or SSH .....	2-97
Subtask L: Enable or Disable OSMS and Host Control .....	2-98
Subtask M: Change User Passwords.....	2-99
Subtask N: Configure Port Binding .....	2-100
Subtask O: Configure Switch Binding .....	2-101
Configuring the Switch Binding Membership List.....	2-104
Subtask P: Configure Fabric Binding .....	2-106
Subtask Q: Enable or Disable Enterprise Fabric Mode....	2-107
Subtask R: Configure OpenTrunking .....	2-108
Subtask S: Install Feature Keys .....	2-111
Task 12: Cable Fibre Channel Ports .....	2-113
Task 13: Configure Zoning.....	2-113
Configure Zones (SANpilot Interface) .....	2-114
Configure Zone Sets (SANpilot Interface) .....	2-117
Task 14: Connect the Director to a Fabric Element.....	2-118
Task 15: Register with the McDATA File Center .....	2-120

## Chapter 3

## Maintenance Analysis Procedures (MAPS)

Maintenance Analysis Procedures.....	3-1
Factory Defaults .....	3-2
Quick Start .....	3-2

MAP 0000: Start MAP .....	3-9
MAP 0100: Power Distribution Analysis .....	3-33
MAP 0200: POST Failure Analysis .....	3-42
MAP 0300: Server Application Problem Determination.....	3-47
MAP 0400: Loss of Server Communication .....	3-56
MAP 0500: FRU Failure Analysis .....	3-74
MAP 0600: Port Card Failure and Link Incident Analysis .....	3-82
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination .....	3-104
MAP 0800: Server Hardware Problem Determination.....	3-121

## Chapter 4      **Repair Information**

Factory Defaults.....	4-2
Procedural Notes .....	4-2
Obtaining Log Information .....	4-3
SAN Management Logs.....	4-4
Element Manager Logs.....	4-6
SANpilot Logs.....	4-11
Obtaining Port Diagnostic Information.....	4-13
Port LEDs.....	4-13
Management Server .....	4-15
SANpilot Interface.....	4-22
Port Properties Page.....	4-28
Performing Port Diagnostic Loopback Tests .....	4-30
Internal Loopback Test (Management Server) .....	4-31
External Loopback Test (Management Server) .....	4-32
Internal Loopback Test (SANpilot Interface).....	4-34
External Loopback Test (SANpilot Interface).....	4-36
Performing Channel Wrap Tests (FICON) .....	4-37
Swapping Ports (FICON) .....	4-38
Collecting Maintenance Data .....	4-39
Management Server .....	4-40
SANpilot Interface.....	4-41
Set the Director Online or Offline.....	4-43
Set Online State (Management Server).....	4-44
Set Offline State (Management Server) .....	4-44
Set Online State (SANpilot Interface) .....	4-45
Set Offline State (SANpilot Interface).....	4-45
Blocking and Unblocking Ports .....	4-46
Block a Port (Management Server).....	4-46
Block a Port Card (Management Server).....	4-47

Unblock a Port (Management Server) .....	4-47
Unblock a Port Card (Management Server) .....	4-48
Block a Port (SANpilot Interface) .....	4-49
Unblock a Port (SANpilot Interface) .....	4-50
Cleaning Fiber-Optic Components .....	4-50
Power-On Procedure .....	4-51
Power-Off Procedure .....	4-52
IML, IPL, or Reset the Director .....	4-53
IML the Director (CTP Front Panel) .....	4-53
IPL the Director (Management Server) .....	4-54
Reset the Director (CTP Front Panel) .....	4-55
Managing Firmware Versions .....	4-55
Management Server .....	4-55
Add a Firmware Version to the Management Server Library .. 4-56	
SANpilot Interface .....	4-66
Managing Configuration Data .....	4-74
Back Up the Configuration .....	4-75
Restore the Configuration .....	4-76
Reset Configuration Data (Management Server) .....	4-77
Reset Configuration Data (SANpilot Interface) .....	4-80
Installing or Upgrading Software .....	4-82

## Chapter 5      **Removal and Replacement Procedures (RRPs)**

Factory Defaults .....	5-1
Procedural Notes .....	5-2
Removing and Replacing FRUs .....	5-2
ESD Information .....	5-3
Concurrent FRUs .....	5-5
Nonconcurrent FRU .....	5-5
RRP: CTP Card .....	5-6
RRP: Port Module Card (UPM and XPM) .....	5-10
RRP: Optical Transceiver (SFP and XFP) .....	5-15
RRP: Filler Panel (UPM and XPM) .....	5-19
RRP: Power Supply .....	5-20
RRP: AC Module .....	5-24
RRP: Fan Module .....	5-27
RRP: Power/System Error LED Assembly .....	5-30
RRP: SBAR Assembly .....	5-31
RRP: Backplane .....	5-35

**Chapter 6      Illustrated Parts Breakdown**

Front-Accessible FRUs .....6-2  
Rear-Accessible FRUs.....6-4  
Miscellaneous Parts.....6-7  
Power Cords and Receptacles.....6-9

**Appendix A      Messages**

Intrepid 6140 Element Manager Messages .....A-1  
    A.....A-1  
    C.....A-3  
    D.....A-13  
    E.....A-15  
    F.....A-17  
    I.....A-18  
    L.....A-24  
    M.....A-24  
    N.....A-25  
    P.....A-26  
    R.....A-28  
    S.....A-29  
    T.....A-30  
    U.....A-34  
    Y.....A-35

**Appendix B      Event Code Tables**

System Events (000 through 199) ..... B-3  
Power Supply Events (200 through 299) ..... B-24  
Fan Module Events (300 through 399) ..... B-28  
CTP Card Events (400 through 499) ..... B-36  
Port Card (UPM and XPM) Events (500 through 599) ..... B-48  
SBAR Events (600 through 699) ..... B-61  
Thermal Events (800 through 899) ..... B-67

**Appendix C      Director Specifications**

Physical Characteristics ..... C-1  
Shipping and Storage Environment ..... C-2  
Operating Environment..... C-2  
Fabriccenter Equipment Cabinet Service Clearances..... C-3

**Appendix D      Management Server and Ethernet Hub**

Management Server Description ..... D-1

Management Server Specifications ..... D-2

Ethernet Hub Description ..... D-2

**Appendix E    Restore Management Server**

Requirements ..... E-1

Restore Management Server Procedure ..... E-2

**Appendix F    Safety Notices (Multi-Lingual Translations)**

**Glossary ..... g-1**

**Index ..... i-1**





1-1	Cabinet-Mounted Intrepid 6140 Directors and Management Server ...	1-3
1-2	Director FRUs (Front Access) .....	1-4
1-3	Director FRUs (Rear Access) .....	1-5
1-4	UPM Card LEDs and Connectors .....	1-8
1-5	XPM Card LEDs and Connectors .....	1-9
1-6	Small Form-Factor Pluggable (SFP) transceiver .....	1-10
1-7	Ten Gbps Form-Factor Pluggable (XFP) Transceiver .....	1-10
1-8	Torque Tool and Hex Adapter .....	1-16
1-9	Door Key .....	1-16
1-10	Loopback Plug .....	1-16
1-11	Fiber-Optic Protective Plug .....	1-17
1-12	Null Modem Cable .....	1-17
2-1	Mounting Bracket Installation (Ethernet Hub) .....	2-10
2-2	Rack Installation (Ethernet Hub) .....	2-10
2-3	Patch Cable and MDI Selector Configuration .....	2-11
2-4	AC Power Connections (Director) .....	2-14
2-5	Connection Description Dialog Box .....	2-16
2-6	COMn Properties Dialog Box .....	2-17
2-7	HyperTerminal Dialog Box .....	2-18
2-8	HyperTerminal Dialog Box .....	2-19
2-9	Management Server Connections .....	2-21
2-10	LCD Panel (New Password) .....	2-23
2-11	LCD Panel (LAN 2 IP Address) .....	2-24
2-12	LCD Panel (LAN 2 Subnet Mask) .....	2-24
2-13	LCD Panel (LAN 1 IP Address) .....	2-25
2-14	LCD Panel (LAN 1 Subnet Mask) .....	2-25
2-15	Welcome to Windows Dialog Box .....	2-26
2-16	Log On to Windows Dialog Box .....	2-27

2-17	EFCM Log In or SANavigator Log In Dialog Box .....	2-27
2-18	Control Panel Window .....	2-28
2-19	Identification Changes Dialog Box .....	2-28
2-20	Internet Protocol (TCP/IP) Properties Dialog Box .....	2-29
2-21	Users and Passwords Dialog Box .....	2-31
2-22	Windows Security Dialog Box .....	2-32
2-23	Change Password Dialog Box .....	2-32
2-24	Add New User Wizard (First Window) .....	2-33
2-25	Add New User Wizard (Second Window) .....	2-33
2-26	Add New User Wizard (Third Window) .....	2-34
2-27	MGMTSERVER\srvacc Properties Dialog Box (General Tab) .....	2-35
2-28	MGMTSERVER\srvacc Properties Dialog Box (Group Membership Tab) 2-35	
2-29	Date/Time Properties Dialog Box (Date & Time Tab) .....	2-36
2-30	Date/Time Properties Dialog Box (Time Zone Tab) .....	2-37
2-31	Call Home Configuration Dialog Box .....	2-38
2-32	Main Window: Example (EFCM or SANavigator) .....	2-40
2-33	EFCM Server or SANavigator Users Dialog Box .....	2-40
2-34	Add User Dialog Box .....	2-41
2-35	Discover Setup Dialog Box .....	2-42
2-36	Domain Information Dialog Box (IP Address Page) .....	2-43
2-37	Configure Feature Key Dialog Box .....	2-45
2-38	New Feature Key Dialog Box .....	2-45
2-39	Install Feature Key Dialog Box .....	2-46
2-40	Configure Date and Time Dialog Box .....	2-50
2-41	Date and Time Synced Dialog Box .....	2-51
2-42	Configure Identification Dialog Box .....	2-52
2-43	Configure Switch Parameters Dialog Box .....	2-54
2-44	Configure Fabric Parameters Dialog Box .....	2-55
2-45	Configure Preferred Paths Dialog Box .....	2-58
2-46	Add Preferred Path Dialog Box .....	2-58
2-47	Switch Binding - Change State Dialog Box .....	2-60
2-48	Switch Binding - Membership List Dialog Box .....	2-61
2-49	Display Options Dialog Box .....	2-62
2-50	Add Detached Node Dialog Box .....	2-63
2-51	Configure Ports Dialog Box .....	2-64
2-52	Configure SNMP Dialog Box .....	2-67
2-53	Configure Threshold Alert(s) Dialog Box .....	2-68
2-54	New Threshold Alerts Dialog Box (Screen 1) .....	2-68
2-55	New Threshold Alerts Dialog Box (Screen 2) .....	2-69
2-56	New Threshold Alerts Dialog Box (Screen 3) .....	2-70
2-57	New Threshold Alerts Dialog Box (Screen 4) .....	2-70
2-58	Configure OpenTrunking Dialog Box .....	2-71

2-59	Email Event Notification Setup Dialog Box .....	2-74
2-60	Configure Ethernet Events Dialog Box .....	2-75
2-61	Configure Call Home Event Notification Dialog Box .....	2-76
2-62	InCD Icon (Unformatted CD) .....	2-79
2-63	Enter Network Password Dialog Box .....	2-83
2-64	SANpilot Interface, View Panel (Director Page) .....	2-83
2-65	Configure Panel (Ports Page) .....	2-84
2-66	Configure BB Credits .....	2-86
2-67	Configure Panel (Director Page with Identification Tab) .....	2-87
2-68	Configure Panel (Director Page with Date/Time Tab) .....	2-88
2-69	Configure Panel (Director Page with Parameters Tab) .....	2-89
2-70	Configure Panel (Director Page with Fabric Parameters Tab) .....	2-91
2-71	Configure Panel (Director Page with Network Tab) .....	2-94
2-72	Configure Panel (Management Page with SNMP Tab) .....	2-96
2-73	Configure Panel (Management Page with CLI Tab) .....	2-97
2-74	Configure Panel (Management Page with OSMS Tab) .....	2-99
2-75	Configure Panel (Security Page with User Rights Tab) .....	2-100
2-76	Configure Panel (Security Page with Port Binding Tab) .....	2-101
2-77	Configure Panel (Security Page with Switch Binding Tab) .....	2-103
2-78	Configure Panel (Security Page with Fabric Binding Tab) .....	2-106
2-79	Configure Panel (Security Page with EFM Tab) .....	2-108
2-80	Configure Panel (Performance Page with OpenTrunking Tab) .....	2-109
2-81	Operations Panel (Feature Installation Tab) .....	2-112
2-82	Configure Panel (Zoning Page with Zones Tab) .....	2-114
2-83	Configure Panel (Zoning Page with Modify Zone Tab) .....	2-116
2-84	Configure Panel (Zoning Page with Zone Set Tab) .....	2-117
2-85	Port Properties Dialog Box .....	2-120
2-86	McDATA File Center Home Page .....	2-120
2-87	McDATA File Center (New User Registration Page) .....	2-122
3-1	Shut Down Windows Dialog Box .....	3-11
3-2	LCD Panel During Boot Sequence .....	3-12
3-3	EFCM Log In or SANavigator Log In Dialog Box .....	3-13
3-4	Main Window: Example (EFCM or SANavigator) .....	3-14
3-5	Port Properties Dialog Box .....	3-19
3-6	Link Incident Log .....	3-20
3-7	Event Log .....	3-21
3-8	Username and Password Required Dialog Box .....	3-25
3-9	SANpilot Interface, View Panel .....	3-26
3-10	SANpilot Interface, View Panel .....	3-28
3-11	SANpilot Interface, View Panel .....	3-30
3-12	SANpilot Interface, Monitor Panel .....	3-32
3-13	Windows Security Dialog Box .....	3-48

3-14	Windows Task Manager Dialog Box (Applications Page) .....	3-49
3-15	Shut Down Windows Dialog Box .....	3-50
3-16	LCD Panel During Boot Sequence .....	3-50
3-17	Dr. Watson for Windows 2000 Dialog Box .....	3-54
3-18	LCD Panel During Boot Sequence .....	3-55
3-19	Ethernet Hubs, Daisy-Chained .....	3-60
3-20	LCD Panel (LAN 2 IP Address) .....	3-64
3-21	Connection Description Dialog Box .....	3-65
3-22	Connect To Dialog Box .....	3-66
3-23	COMn Properties Dialog Box .....	3-66
3-24	Intrepid 6140 - HyperTerminal Dialog Box .....	3-67
3-25	HyperTerminal Dialog Box .....	3-68
3-26	HyperTerminal Dialog Box .....	3-68
3-27	Discover Setup Dialog Box .....	3-69
3-28	Editing Domain Information Dialog Box .....	3-69
3-29	Domain Information Dialog Box (IP Address Page) .....	3-70
3-30	EFCM or SANavigator Message Dialog Box .....	3-71
3-31	Domain Information Dialog Box (IP Address Page) .....	3-71
3-32	UPM Card Diagram (Front) .....	3-85
3-33	UPM Card Diagram (Rear) .....	3-85
3-34	Configure Fabric Parameters Dialog Box .....	3-92
3-35	Switch Binding - State Change Dialog Box .....	3-95
3-36	Fabric Binding Dialog Box .....	3-96
3-37	Switch Binding - Membership List Dialog Box .....	3-97
3-38	Clear Link Incident Alert(s) .....	3-98
3-39	UPM Card Diagram (Front) .....	3-103
3-40	UPM Card Diagram (Rear) .....	3-104
3-41	Configure Fabric Parameters Dialog Box .....	3-111
3-42	Configure Switch Parameters Dialog Box .....	3-112
3-43	Zoning Dialog Box (Zone Library Tab) .....	3-113
3-44	Zoning Dialog Box (Active Zone Set Tab) .....	3-114
3-45	EFCM or SANavigator Message Dialog Box .....	3-122
3-46	Windows Task Manager Dialog Box .....	3-123
3-47	Shut Down Windows Dialog Box .....	3-124
3-48	LCD Panel During Boot Sequence .....	3-124
3-49	EFCM Log In or SANavigator Log In Dialog Box .....	3-125
3-50	LCD Panel During Boot Sequence .....	3-127
4-1	Event Log .....	4-4
4-2	Product Status Log .....	4-5
4-3	Intrepid 6140 Event Log .....	4-6
4-4	Intrepid 6140 Hardware Log .....	4-8
4-5	Intrepid 6140 Link Incident Log .....	4-9

4-6	Intrepid 6140 Threshold Alert Log .....	4-10
4-7	Intrepid 6140 Open Trunking Log .....	4-11
4-8	SANpilot Logs .....	4-12
4-9	Port List View .....	4-15
4-10	Performance View .....	4-17
4-11	Port Properties Dialog Box .....	4-20
4-12	Port Technology Dialog Box .....	4-22
4-13	Monitor Panel (Port List Page) .....	4-23
4-14	Monitor Panel (Port Stats Page) .....	4-24
4-15	View Panel (Port Properties Page) .....	4-29
4-16	Port Diagnostics Dialog Box .....	4-31
4-17	Operations Panel (Port Page with Diagnostics Tab) .....	4-35
4-18	Swap Ports Dialog Box .....	4-39
4-19	Save Data Collection Dialog Box .....	4-40
4-20	Data Collection Dialog Box .....	4-41
4-21	Operations Panel (Maintenance Page with System Files Tab) .....	4-42
4-22	Save As Dialog Box .....	4-42
4-23	Download Complete Dialog Box .....	4-43
4-24	Set Online State Dialog Box .....	4-44
4-25	Operations Panel (Switch Page with Online State Tab) .....	4-45
4-26	Blocking Port Warning Box .....	4-46
4-27	Unblocking Port Warning Box .....	4-48
4-28	Configure Panel (Ports Page) .....	4-49
4-29	Clean Fiber-Optic Components .....	4-51
4-30	Information Dialog Box .....	4-54
4-31	Firmware Library Dialog Box .....	4-56
4-32	McDATA File Center Home Page .....	4-57
4-33	McDATA File Center (Login Page) .....	4-58
4-34	McDATA File Center (Find Documents Page) .....	4-58
4-35	McDATA File Center (Documents Match Page) .....	4-59
4-36	McDATA File Center (Current Request Page) .....	4-59
4-37	McDATA File Center (Request History Page) .....	4-60
4-38	File Download Dialog Box .....	4-60
4-39	Save As Dialog Box .....	4-61
4-40	Download Complete Dialog Box .....	4-61
4-41	Firmware Library Dialog Box .....	4-62
4-42	New Firmware Version Dialog Box .....	4-62
4-43	New Firmware Description Dialog Box .....	4-63
4-44	File Transfer Message Box .....	4-63
4-45	Firmware Library Dialog Box .....	4-64
4-46	Warning Dialog Box .....	4-65
4-47	Send Firmware Dialog Box .....	4-66
4-48	View Panel (Unit Properties Page) .....	4-66

4-49	McDATA File Center Home Page .....	4-67
4-50	McDATA File Center (Login Page) .....	4-68
4-51	McDATA File Center (Find Documents Page) .....	4-68
4-52	McDATA File Center (Documents Match Page) .....	4-69
4-53	McDATA File Center (Current Request Page) .....	4-69
4-54	McDATA File Center (Request History Page) .....	4-70
4-55	File Download Dialog Box .....	4-71
4-56	Save As Dialog Box .....	4-71
4-57	Download Complete Dialog Box .....	4-72
4-58	Operations Panel (Maintenance Page with Firmware Upgrade Tab) .	4-73
4-59	Browser-Specific Message Box .....	4-73
4-60	Firmware Received Message Box .....	4-74
4-61	Firmware Upgrade Complete Message Box .....	4-74
4-62	Backup and Restore Configuration Dialog Box .....	4-75
4-63	Information Dialog Box .....	4-76
4-64	Backup and Restore Configuration Dialog Box .....	4-76
4-65	Warning Dialog Box .....	4-77
4-66	Restore Dialog Box .....	4-77
4-67	Reset Configuration Dialog Box .....	4-78
4-68	Discover Setup Dialog Box .....	4-79
4-69	Domain Information Dialog Box .....	4-79
4-70	Operations Panel (Switch Page with Reset Config Tab) .....	4-81
4-71	Browser-Specific Message Box .....	4-81
4-72	McDATA File Center Home Page .....	4-83
4-73	McDATA File Center (Find Documents Page) .....	4-84
4-74	McDATA File Center (Documents Match Page) .....	4-84
4-75	McDATA File Center (Current Request Page) .....	4-85
4-76	McDATA File Center (Request History Page) .....	4-85
4-77	File Download Dialog Box .....	4-86
4-78	Save As Dialog Box .....	4-86
4-79	Download Complete Dialog Box .....	4-87
4-80	Run Dialog Box .....	4-87
4-81	McDATA EFC Management Applications Dialog Box .....	4-88
4-82	SANavigator Log In or EFCM Log In Dialog Box .....	4-89
5-1	ESD Grounding Points .....	5-4
5-2	CTP Card Removal and Replacement .....	5-7
5-3	UPM Card Removal and Replacement .....	5-13
5-4	SFP Optical Transceiver Removal and Replacement .....	5-17
5-5	Filler Panel Removal and Replacement .....	5-20
5-6	Power Supply Removal and Replacement .....	5-22
5-7	AC Module Removal and Replacement .....	5-25
5-8	Fan Module Removal and Replacement .....	5-28

5-9	Power/System Error LED Assembly Removal and Replacement .....	5-31
5-10	SBAR Assembly Removal and Replacement .....	5-33
5-11	Backplane Removal and Replacement .....	5-37
6-1	Front-Accessible FRUs .....	6-2
6-2	Rear-Accessible FRUs (Part 1) .....	6-4
6-3	Rear-Accessible FRUs (Part 2) .....	6-6
6-4	Miscellaneous Parts .....	6-7
6-5	Power Cords and Receptacles .....	6-9
D-1	Management Server .....	D-1
D-2	24-Port Ethernet Hub .....	D-3
E-1	Run Dialog Box .....	E-4
E-2	VNC Authentication Screen .....	E-5
E-3	Welcome to Windows Dialog Box .....	E-5
E-4	Log On to Windows Dialog Box .....	E-6
E-5	EFCM Log In or SANavigator Log In Log In Dialog Box .....	E-6





1-1	Element Manager Alert Symbols, Messages, and Status .....	1-14
2-1	Factory-Set Defaults (Intrepid 6140 Director) .....	2-1
2-2	Factory-Set Defaults (Management Server) .....	2-2
2-3	Installation Task Summary .....	2-4
2-4	Factory-Set Defaults (Intrepid 6140 Director) .....	2-15
2-5	Element Manager Alert Symbols, Messages, and Status .....	2-44
2-6	Code Page Table .....	2-48
3-1	Factory-Set Defaults .....	3-2
3-2	MAP Summary .....	3-2
3-3	Event Codes versus Maintenance Action .....	3-3
3-4	MAP 100: Event Codes .....	3-34
3-5	MAP 200: Event Codes .....	3-43
3-6	MAP 200: Byte 0 FRU Codes .....	3-44
3-7	MAP 400: Event Codes .....	3-57
3-8	MAP 400: Error Messages .....	3-59
3-9	MAP 500: Event Codes .....	3-74
3-10	MAP 600: Event Codes .....	3-83
3-11	Port Operational and LED States (Management Server) .....	3-87
3-12	Port Properties, Invalid Attachment Reasons and Actions .....	3-90
3-13	MAP 600: Port Operational States and Actions (SANpilot) .....	3-102
3-14	MAP 700: Event Codes .....	3-105
3-15	Port Segmentation Reasons and Actions (Management Server) .....	3-106
3-16	Byte 4, Segmentation Reasons, and Actions .....	3-109
3-17	Bytes 8 through 11 Failure Reasons and Actions .....	3-118
3-18	Segmentation Reasons and Actions (SANpilot) .....	3-120
4-1	Factory-Set Defaults .....	4-2

4-2	Port Operational States .....	4-13
5-1	Factory-Set Defaults .....	5-1
5-2	Concurrent FRUs .....	5-5
5-3	Nonconcurrent FRU .....	5-5
6-1	Front-Accessible FRU Parts List .....	6-3
6-2	Rear-Accessible FRU Parts List (Part 1) .....	6-5
6-3	Rear-Accessible FRU Parts List (Part 2) .....	6-6
6-4	Miscellaneous Parts .....	6-8
6-5	Power Cord and Receptacle List .....	6-10

---

## Preface

---

---

*This publication is part of a documentation suite that supports the  
McDATA® Intrepid® 6140 (ED-6140) Director.*

### **Who Should Use This Manual**

This publication is intended for use by installation and service representatives experienced with the director, storage area network (SAN) technology, and Fibre Channel technology.

### **Organization of This Manual**

This publication includes six chapters and four appendices organized as follows:

[Chapter 1, General Information](#). This chapter describes the maintenance approach to director problem analysis and repair. The chapter provides a description of the director and associated Enterprise Fabric Connectivity (EFC) Server, specifications, remote workstation configurations and minimum specifications, field-replaceable units (FRUs), switches, connectors, and indicators, software diagnostic features, and tools and test equipment.

[Chapter 2, Installation Tasks](#). This chapter describes tasks to install, configure, and verify operation of the director and management server. The director can be installed on a desktop, mounted in a McDATA-supplied FC-512 Fabricenter® equipment cabinet, or mounted in any standard 19-inch equipment rack.

[Chapter 3, \*Maintenance Analysis Procedures \(MAPS\)\*](#). This chapter describes maintenance analysis procedures (MAPs) to fault isolate a director problem to an individual FRU.

[Chapter 4, \*Repair Information\*](#). This chapter describes supplementary diagnostic and repair procedures for a failed director. The chapter includes procedures to display and use log information, perform port diagnostics, manage configuration data, collect maintenance data, power-on, power-off, and initial program load (IPL) the director, set the director online or offline, block ports, manage director firmware, clean fiber optics, and install or upgrade management server software.

[Chapter 5, \*Removal and Replacement Procedures \(RRPs\)\*](#). This chapter describes procedures to remove and replace director FRUs.

[Chapter 6, \*Illustrated Parts Breakdown\*](#). This chapter illustrates, describes, and shows the location of director FRUs. In addition, FRUs are cross-referenced to corresponding part numbers.

[Appendix A, \*Messages\*](#) This appendix provides a list of user and error messages that appear at the EFC Manager and ED-6140 Element Manager applications at the management server. A description of each message and a recommended course of action in response to the message are also provided.

[Appendix B, \*Event Code Tables\*](#) This appendix provides an explanation of event codes that appear at the Element Manager application. The event severity and a recommended course of action in response to each event are also provided.

[Appendix C, \*Director Specifications\*](#). This appendix provides the director specifications including its physical characteristics, and storage, shipping, and operating environments.

[Appendix D, \*Management Server and Ethernet Hub\*](#). This appendix provides the management-server specifications and a description of the ethernet hub.

[Appendix E, \*Restore Management Server\*](#) This appendix provides the instructions to restore all required director applications to the management server in case of a hard drive failure.

[Appendix D, \*Consolidating Management Servers\*](#) This appendix provides the instructions consolidate operation and network addressing of multiple management servers.

[Appendix F, \*Safety Notices \(Multi-Lingual Translations\)\*](#). This appendix provides the translation of the safety notices in this publication.

A [Glossary](#) defines terms, abbreviations, and acronyms used in the manual. An [Index](#) is also provided.

## Related Publications

Other publications that provide additional information about the director include:

- *McDATA Products in a SAN Environment Planning Manual* (620-000124).
- *McDATA Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153).
- *McDATA Enterprise Fabric Connectivity Manager User Manual* (620-005001).
- *McDATA SANpilot User Manual* (620-000160).
- *McDATA SNMP Support Manual* (620-000131).
- *McDATA E/OS Command Line Interface User Manual* (620-000134).
- *McDATA Rack-Mount Kit, Intrepid 6140 Director in Fabriccenter (FC-512) Cabinet, Installation Instructions* (958-000317).
- *McDATA EFCM Lite Installation Instructions* (958-000171).
- *1U Server Rack-Mount Kit Installation Instructions* (958-000310).
- *SANavigator User Guide* (621-000013).
- *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100).

## Ordering Printed Manuals

To order a paper copy of this manual, submit a purchase order as described in *Ordering McDATA Documentation Instructions*, which is found on McDATA's web site, <http://www.mcdata.com>. To obtain documentation CD-ROMs, contact your sales representative.

**Where to Get Help**

For technical support, contact the McDATA Solution Center. The center provides a single point of contact, and is staffed 24 hours a day, seven days a week, including holidays. Contact the center at the phone number, fax number, or e-mail address listed below. Please have the product serial number (printed on the service label attached to the director) available.

**Phone: (800) 752-4572 or (720) 558-3910**

**Fax: (720) 558-3851**

**E-mail: [support@mcddata.com](mailto:support@mcddata.com)**

**Forwarding  
Publication  
Comments**

We welcome comments about this publication. Please send comments to the McDATA Solution Center by telephone, fax, or e-mail. The numbers and e-mail address are listed above. Please identify the manual, page numbers, and details.

**Trademarks**

The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation or SANavigator, Inc. in the United States or other countries or both:

**Registered Trademarks**

McDATA®

Intrepid®

Fabricenter®

OPENready®

SANpilot®

SANtegrity®

**Trademarks**

Sphereon™

Fibre Channel Director™

SANavigator®HotCAT™

OPENconnectors™

EON™

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States or other countries or both.

**Laser Compliance  
Statement**

Laser transceivers for the ED-6140 Director are tested and certified in the United States to conform to Title 21 of the Code of Federal Regulations (CFR), Subchapter J, Parts 1040.10 and 1040.11 for Class 1 laser products. Elsewhere, the transceivers are tested and certified to be compliant with International Electrotechnical Commission IEC825-1 and European Norm EN60825-1 and EN60825-2 regulations for Class 1 laser products. Class 1 laser products are not considered

hazardous. The transceivers are designed such that there is never human access to laser radiation above a Class 1 level during normal operation or prescribed maintenance conditions.

**Federal  
Communications  
Commission (FCC)  
Statement**

The director generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions provided, may cause interference to radio communications. The directors have been tested and found to comply with the limits for Class A computing devices pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her own expense, will take whatever measures are required to correct the interference. Any modifications or changes made to the ED-6140 without explicit approval from McDATA, by means of a written endorsement or through published literature, will invalidate the service contract and void the warranty agreement with McDATA.

**Chinese Class A  
Telecommunication  
Product Statement**

**警告使用者：**

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

**European Union  
Conformity  
Declarations for  
Information  
Technology  
Equipment**

The ED-6140 Director meets the following regulatory requirements as set forth by European Norms (ENs) and International Electrotechnical Commission (IEC) standards for commercial and light industrial information technology equipment (ITE).

- **EN55022: 1998; EN55024: 1997, +A1: 1998:** ITE-generic radio frequency interference (RFI) emission standard for domestic, commercial, and light industrial environments.
- **EN60950:** ITE-generic electrical and fire safety standard for domestic, commercial, and light industrial environments.

**European Union  
Directives**

The European Union (EU) Council has implemented a series of directives that define product safety standards for all EU member countries. The following directives apply to the ED-6140 Director:

- The director conforms with all protection requirements of EU directive 89/336/EEC (EMC Directive) in accordance with of the laws of the member countries relating to electromagnetic compatibility (EMC), emissions, and immunity.
- The director conforms with all protection requirements of EU directive 73/23/EEC (Low Voltage Directive) in accordance with of the laws of the member countries relating to electrical safety.
- The director conforms with all protection requirements of EU directive 93/68/EEC (Machinery Directive) in accordance with of the laws of the member countries relating to safe electrical and mechanical operation of the equipment.

McDATA does not accept responsibility for any failure to satisfy the protection requirements of any of these directives resulting from a non-recommended or non-authorized modification to the switch.

## Dangers and Cautions

The following **DANGER** statements appear in this publication and describe safety practices that must be observed while installing or servicing the director. A **DANGER** statement provides essential information or instructions for which disregard or noncompliance may result in death or severe personal injury.



### **DANGER**

*Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.*



### **DANGER**

*Disconnect the power cords.*

The following **CAUTION** statements appear in this publication and describe safety practices that must be observed while installing or servicing the director. A **CAUTION** statement provides essential information or instructions for which disregard or noncompliance may result in personal injury.



**CAUTION**

**Use safe lifting practices when moving the product.**

**General Precautions**

When installing or servicing the director, follow these practices:

- Always use correct tools.
- Always use correct replacement parts.
- Keep all paperwork up to date, complete, and accurate.

**ESD Precautions**

The director contains electrostatic discharge (ESD) sensitive FRUs. When working with any director FRU, always use correct ESD procedures.

- Always wear a wrist grounding strap connected to chassis ground (if the director is plugged in) or a bench ground.
- Always store ESD-sensitive components in antistatic packaging.



The McDATA® Intrepid® 6140 Director provides up to 140 ports of high-performance, dynamic Fibre Channel connectivity for switched fabric devices in a storage area network (SAN). The director provides a broad bandwidth (2 or 10 gigabits per second), redundant switched data paths, and long transmission distances.

This chapter presents information and features of the director and its management, including:

- Director description.
- Field-replaceable units (FRUs).
- Error detection, reporting, and serviceability features.
- Element Manager status indicators
- Tools and test equipment.
- Director management.

## Director Description

The Intrepid 6140 Director is a 140-port product that provides dynamic switched connections between Fibre Channel servers and devices in a SAN environment. The ports operate at 2 or 10 gigabits per second (Gbps). Directors (from one to three) can be configured to order in a McDATA-supplied FC-512 Fabriccenter™ equipment cabinet, which can provide up to 420 ports in a single cabinet.

The director provides dynamic switched connections for servers and devices, supports mainframe and open-systems interconnection (OSI)

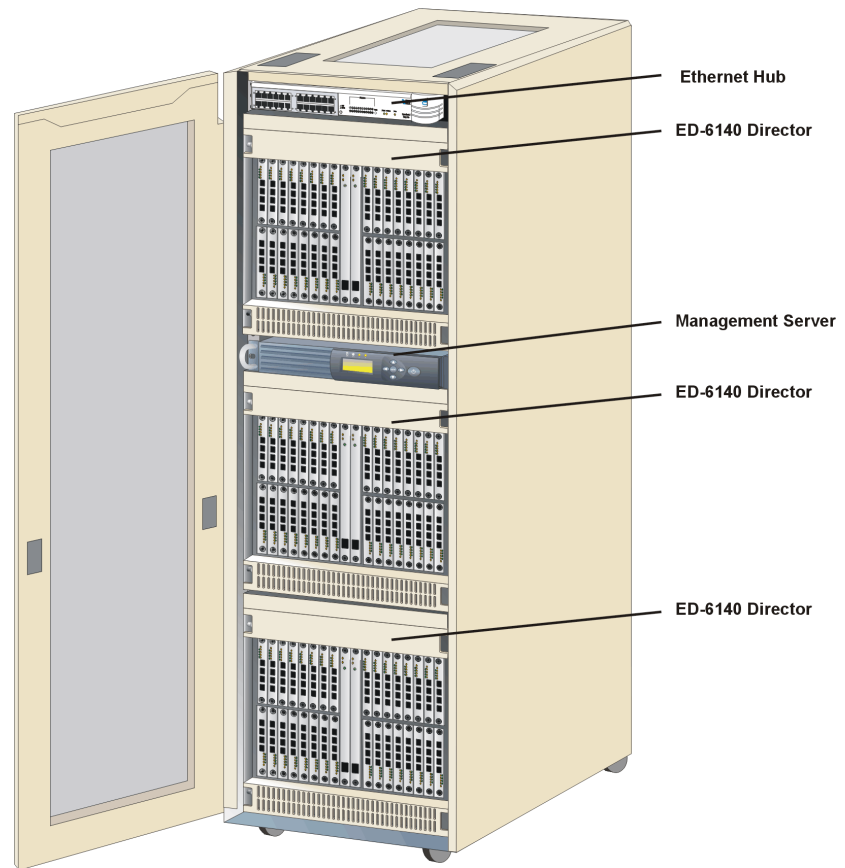
computing environments, and provides data transmission and flow control between device node ports (N\_Ports) as dictated by the *Fibre Channel Physical and Signaling Interface* (FC-PH 4.3). Through interswitch links (ISLs), the director can also connect to one or more additional directors to form a Fibre Channel multiswitch fabric.

The director can be managed through a rack-mount management server running a Java™-based SAN management application (SANavigator® or Enterprise Fabric Connectivity Manager (EFCM)) and the Intrepid 6140 Element Manager application.

Multiple directors and the management server communicate on a local area network (LAN) through one or more 10/100 Base-T Ethernet hubs. One or more 24-port Ethernet hubs are optional and can be ordered with the director. Up to three hubs can be daisy-chained to provide additional Ethernet connections as more directors (or other McDATA managed products) are installed on a customer network.

As an option, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the director through the SANpilot interface. The SANpilot interface manages only a single director, and provides a graphical user interface (GUI) that supports product configuration, statistics monitoring, and basic operation. The SANpilot interface is opened from a standard web browser running Netscape Navigator® 4.6 or higher or Microsoft® Internet Explorer 4.0 or higher.

[Figure 1-1](#) illustrates an equipment rack with three directors, the management server, and an Ethernet hub.



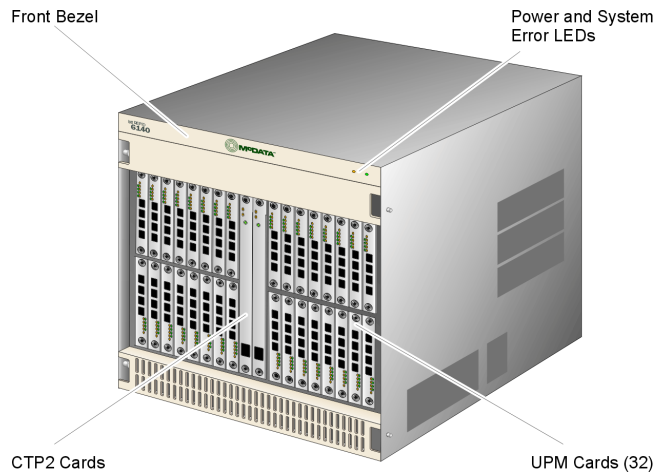
**Figure 1-1 Cabinet-Mounted Intrepid 6140 Directors and Management Server**

## Field-Replaceable Units

The director provides a modular design that enables quick removal and replacement of FRUs. This section describes director FRUs and controls, connectors, and indicators associated with the FRUs.

Director FRUs accessed from the front (Figure 1-2) include the:

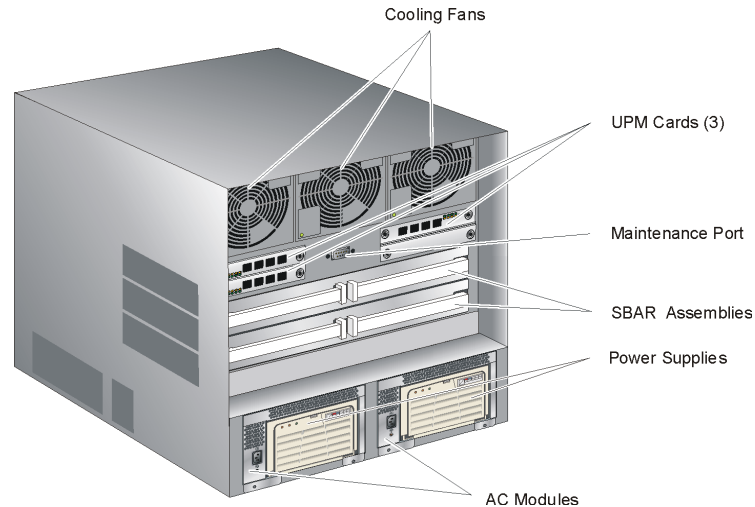
- Universal port module (UPM) cards (2 Gbps).
- 10 Gbps port module (XPM) cards.
- Control processor (CTP) cards.



**Figure 1-2 Director FRUs (Front Access)**

Director FRUs accessed from the rear (Figure 1-3) include the:

- Fan modules.
- Universal port module (UPM) cards (2 Gbps).
- 10 Gbps port module (XPM) cards.
- Serial crossbar (SBAR) assemblies.
- Power supplies.
- AC modules.
- Power/System Error LED Assembly (not shown).
- Backplane (not shown).



**Figure 1-3 Director FRUs (Rear Access)**

## Power/System LED Assembly

The bezel at the top front of the director includes an amber system error light-emitting diode (LED) and a green power LED. These LEDs are actuated and controlled by a Power/System LED Assembly which is accessed from the rear of the director.

The power LED illuminates when the director is powered on and operational. If the LED extinguishes, a facility power source, alternating current (AC) power cord, or director power distribution failure is indicated.

The system error LED illuminates when the director detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when the *Clear System Error Light* function is selected from the Element Manager application. The LED blinks if unit beaconing is enabled. An illuminated system error LED (indicating a failure) takes precedence over unit beaconing.

## CTP Card

The director is delivered with two CTP cards. The active CTP card initializes and configures the director after power on and contains the microprocessor and associated logic that coordinate director operation.

The CTP card provides an initial machine load (IML) button and a **RESET** button (recessed) on the faceplate.

When the **IML** button is pressed, held for three seconds, and released, the director performs an IML that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic.

When the **RESET** button is pressed and held for three seconds, the director performs a reset. A reset is disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during director reset must be retransmitted.

A reset should only be performed if a CTP card failure is indicated. As a precaution, the **RESET** button is flush mounted to protect against inadvertent activation.

Each CTP card also provides a 10/100 megabit per second (Mbps) RJ-45 twisted pair connector on the faceplate that attaches to an Ethernet local area network (LAN) to communicate with the management server or a simple network management protocol (SNMP) management station.

Each CTP card provides system services processor (SSP) and embedded port (EP) subsystems. The SSP subsystem runs director applications and the underlying operating system, communicates with director ports, and controls the RS-232 maintenance port and 10/100 Mbps Ethernet port. The EP subsystem provides Class F and exception frame processing, and manages frame transmission to and from the SBAR assembly. In addition, a CTP card provides nonvolatile memory for storing firmware, director configuration information, persistent operating parameters, and memory dump files. Director firmware is upgraded concurrently (without disrupting operation).

The backup CTP card takes over operation if the active card fails. Failover from a faulty card to the backup card is transparent to attached devices.



Each card faceplate contains a green LED that illuminates if the card is operational and active, and an amber LED that illuminates if the card fails. Both LEDs are extinguished on an operational backup card. The amber LED blinks if FRU beaconing is enabled.

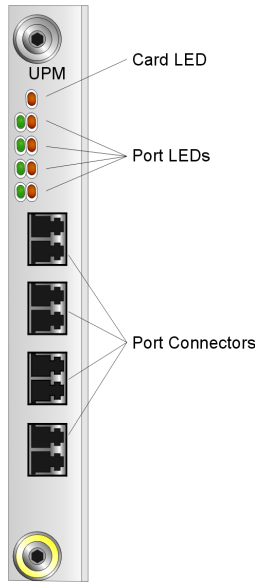
---

## UPM Card

Each UPM card (Figure 1-4) provides four full-duplex generic ports (G\_Ports) that transmit or receive data at 2 gigabits per second (Gbps). G\_Port functionality depends on the type of cable attachment. UPM cards use non-open fiber control (OFC) Class 1 laser transceivers that comply with Section 21 of the Code of Federal Regulations (CFR), Subpart (J) as of the date of manufacture.

The card faceplate contains:

- Four duplex LC connectors for attaching fiber-optic cables.
- An amber LED (at the top of the card) that illuminates if any port fails or blinks if FRU beaconing is enabled.
- A bank of amber and green LEDs above the ports. One amber LED and one green LED are associated with each port and indicate port status as follows:
  - The green LED illuminates (or blinks if there is active traffic) and the amber LED extinguishes to indicate normal port operation.
  - The amber LED illuminates and the green LED extinguishes to indicate a port failure.
  - Both LEDs extinguish to indicate a port is operational but not communicating with an N\_Port (no cable attached, loss of light, port blocked, or link recovery in process).
  - The amber LED flashes and the green LED either remains on, extinguishes, or flashes to indicate a port is beaconing or running online diagnostics.

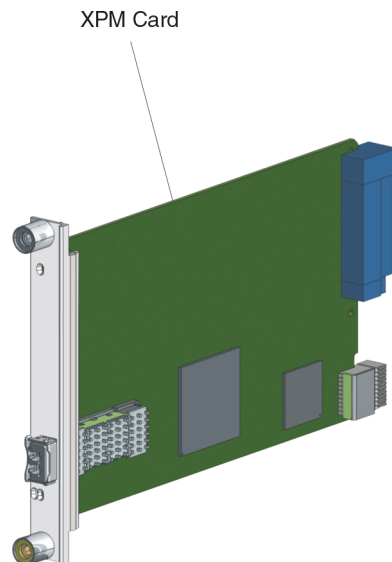


**Figure 1-4 UPM Card LEDs and Connectors**

## XPM Card

Each XPM card ([Figure 1-5](#)) provides one full-duplex generic port (G\_Port) that transmits or receives data at 10 gigabits per second (Gbps). The card faceplate contains:

- One duplex LC connector for attaching fiber-optic cables.
- Amber and green LEDs that indicate port status similar to the LEDs on the UPM cards ([UPM Card](#) on page 1-7).



**Figure 1-5 XPM Card LEDs and Connectors**

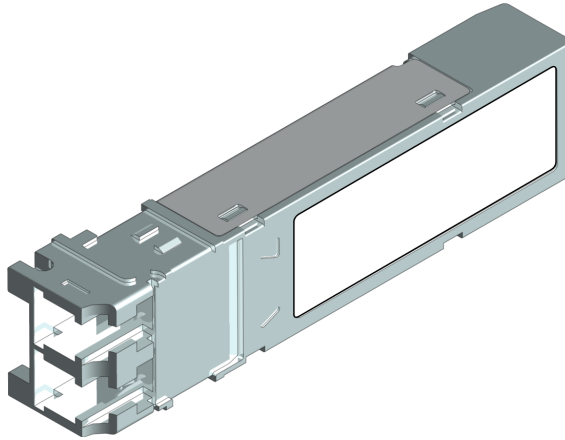
## SFP and XFP Transceivers

Singlemode or multimode fiber-optic cables attach to director ports through 2 Gbps small form-factor pluggable (SFP, [Figure 1-6](#) - for UPM cards) or 10 Gbps form-factor pluggable (XFP, [Figure 1-7](#) - for XPM cards) optic transceivers. The fiber-optic transceivers provide duplex LC<sup>®</sup> connectors and can be detached from director ports for easy replacement.

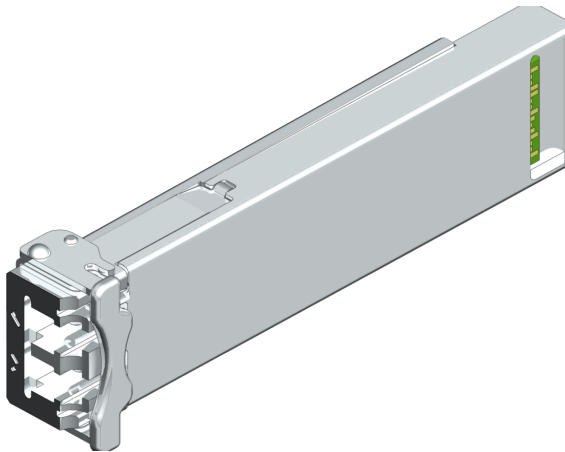
**NOTE:** SFP and XFP transceivers are not interchangeable.

These fiber-optic transceiver types are available:

- Shortwave laser, SFP, 2.125 Gbps
- Shortwave laser, XFP, 10.625 Gbps
- Longwave laser, SFP, 2.125 Gbps
- Longwave laser, XFP, 10.625 Gbps



**Figure 1-6 Small Form-Factor Pluggable (SFP) transceiver**



**Figure 1-7 Ten Gbps Form-Factor Pluggable (XFP) Transceiver**

---

## Power Supply

Redundant, load-sharing power supplies step down and rectify facility input power to provide 48-volt direct current (VDC) power to director FRUs. The power supplies also provide overvoltage and overcurrent protection. Either power supply can be replaced while the director is powered on and operational.

Each power supply has a separate backplane connection to allow for different AC power sources. The power supplies are input rated at 180 to 264 volts alternating current (VAC). The faceplate of each power supply provides the following status LEDs:

- A green **AC OK** LED illuminates if the power supply is operational and receiving AC power.
- A green **DC OK** LED illuminates if the power supply is operational and producing DC power.
- A red **FAULT** LED illuminates if the power supply fails.

---

## AC Module

The AC module is located at the bottom rear of the director. Either AC module can be replaced while the director is powered on and operational. The module provides:

- Two single-phase, 220 VAC, power connectors.
- An input filter and AC system harness (internal to the FRU) that provides the wiring to connect the AC power connectors to the power supplies (through the backplane).

---

## Fan Module

Three fan modules, each containing one system fan (three system fans total), provide cooling for director FRUs, as well as redundancy for continued operation if a fan fails.

A fan module can be replaced while the director is powered on and operating, provided the module is replaced within ten minutes (after which software powers off the director). An amber LED for each fan module illuminates if one or more fans fail or rotate at insufficient angular velocity.

---

## SBAR Assembly

The director is delivered with two SBAR assemblies. The active SBAR is responsible for Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention. The assembly accepts a connection request from a port, determines if a connection can be established, and establishes the connection if the destination port is available. The assembly also stores busy, source connection, and error status for each director port.

The backup SBAR takes over operation if the active assembly fails, and provides the ability to maintain connectivity and data frame

transmission without interruption. Failover to the backup assembly is transparent to attached devices.

Each SBAR assembly consists of a card and steel carriage that mounts flush on the backplane. The carriage provides protection for the back of the card, distributes cooling airflow, and assists in aligning the assembly during installation. The rear of the carriage contains a green LED that illuminates if the assembly is operational and active, and an amber LED that illuminates if the assembly fails. Both LEDs are extinguished on an operational backup assembly. The amber LED blinks if FRU beaconing is enabled.

---

## Backplane

The backplane provides 48 VDC power distribution and connections for all logic cards. The backplane is a nonconcurrent FRU. The director must be powered off prior to FRU removal and replacement.

---

## Error-Detection, Reporting, and Serviceability Features

The director provides the following error detection, reporting, and serviceability features:

- Light-emitting diodes (LEDs) on director FRUs and the front bezel that provide visual indicators of hardware status or malfunctions.
- Redundant FRUs (logic cards, power supplies, and cooling fans) that are removed or replaced without disrupting director or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without the use of special tools or equipment.
- System alerts and logs that display director, Ethernet link, and Fibre Channel link status at the management server (running a SAN management application), client communicating with the management server, or SANpilot interface.
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (internal loopback, external loopback, and Fibre Channel (FC) wrap tests). The FC wrap test applies only when the director is configured to operate in FICON management style.

- An RS-232 maintenance port at the rear of the director (port access is password protected) that enables installation or service personnel to change the director's internet protocol (IP) address, subnet mask, and gateway address; or to run diagnostics and isolate system problems through a local or remote terminal.

The director parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the director.

- Data collection through the Element Manager application or the SANpilot interface to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Beaconing to assist service personnel in locating a specific port, FRU, or director in a multiswitch environment. When port beaconing is enabled, the amber LED associated with the port flashes. When FRU beaconing is enabled, the amber (service required) LED on the FRU flashes. When unit beaconing is enabled, the system error indicator on the front bezel flashes. Beaconing does not affect port, FRU, or director operation.
- An internal modem for use by support personnel to dial-in to the management server for event notification and to perform remote diagnostics.
- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.

---

**NOTE:** The call-home feature is not available through the SANpilot interface. The call-home feature may not be available if the EFCM Lite application is installed on a customer-supplied platform.

---

- Concurrent port maintenance. UPM and XPM cards are added or replaced and fiber-optic cables are attached to ports without interrupting other ports or director operation.
- Status monitoring of redundant FRUs and alternate Fibre Channel data paths to ensure continued director availability in case of failover. The SAN management application queries the status of each backup FRU. A backup FRU failure is indicated by an illuminated amber LED.

- SNMP management using the Fibre Channel Fabric Element MIB (Version 1.1), transmission control protocol/internet protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on each director. Up to six authorized management workstations can be configured through the Element Manager application or SANpilot interface to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.
- SNMP management using the Fibre Alliance MIB (Version 3.1) that runs on the management server. Up to 12 authorized management workstations can be configured through the SAN management application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

## Element Manager Status Indicators

In addition to the visual indicators on the director chassis, the Element Manager application presents alert symbols and messages that describe the condition of the director and its FRUs. These alert symbols, messages, and a description are summarized in [Table 1-1](#).

**Table 1-1 Element Manager Alert Symbols, Messages, and Status**





Symbol	Message	Description
	Fully operational	All components and installed ports are operational.
	Redundant failure	A redundant component has failed, and the backup component has taken over.
	Minor failure	A failure has occurred that has decreased the director operational capability, but has not affected normal switching operations.
	Major failure	Power supplies have failed.



Table 1-1 Element Manager Alert Symbols, Messages, and Status (*continued*)

Symbol	Message	Description
	Loading firmware	The system is busy loading new firmware, but the system is otherwise operational.
	Not operational	A critical failure has occurred that prevents the director from performing fundamental switching operations.
	<ul style="list-style-type: none"> <li>o Link time-out</li> <li>o Protocol mismatch</li> <li>o Never connected</li> </ul>	Director status is unknown. Occurs is network connection between the management server and the director is lost, or if a CTP card fails and there is no operational backup, or if there is no system power.

## Tools and Test Equipment

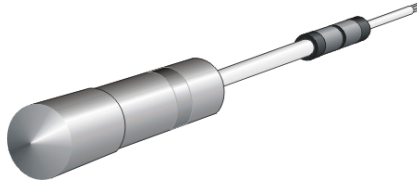
This section describes tools and test equipment that may be required to test, service, and verify operation of the director and attached management server. These tools are either supplied with the director or must be supplied by service personnel.

### Tools Supplied with the Director

The following tools are supplied with the director. Use of the tools may be required to perform installation, test, service, or verification tasks.

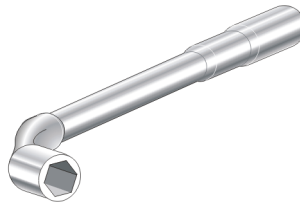
- **Torque tool with hexagonal adapter** - The torque tool with 5/32" hexagonal adapter ([Figure 1-8](#)) is required to remove and replace director logic cards.

**ATTENTION!** The torque tool supplied with the Intrepid 6140 Director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another McDATA product. Use of the wrong tool may overtighten and damage logic cards.



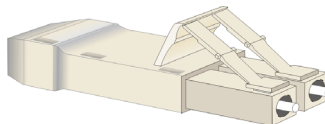
**Figure 1-8 Torque Tool and Hex Adapter**

- **Door key** - The door key with 5/16" socket ([Figure 1-9](#)) is required to open the front or rear door of the FC-512 Fabriccenter equipment cabinet. A 5/16" socket wrench may be used in lieu of the door key.



**Figure 1-9 Door Key**

- **Loopback plug** - An SFP multimode (shortwave laser) or singlemode (longwave laser) loopback plug ([Figure 1-10](#)) is required to perform port loopback diagnostic tests. One loopback plug is shipped with the director, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed.



**Figure 1-10 Loopback Plug**

- **Fiber-optic protective plug** - For safety and port transceiver protection, fiber-optic protective plugs ([Figure 1-11](#)) must be inserted in all director ports without fiber-optic cables attached. The director is shipped with protective plugs installed in all ports.

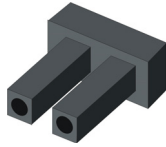


Figure 1-11 Fiber-Optic Protective Plug

- **Null modem cable** - An asynchronous RS-232 null modem cable (Figure 1-12) is required to configure director network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors.

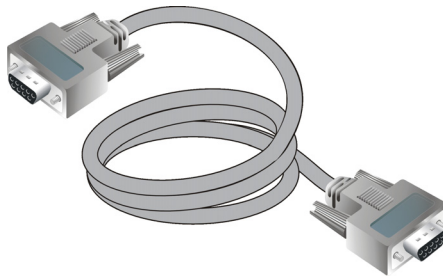


Figure 1-12 Null Modem Cable

### Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing director installation or maintenance actions. Use of the tools may be required to perform one or more test, service, or verification tasks.

- **Scissors or pocket knife** - A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers** - Screwdrivers are required to remove, replace, adjust or tighten various FRUs, chassis, or cabinet components.
- **T10 Torts® tool** - The tool is required to rack-mount the director or to remove, replace, adjust or tighten various chassis or cabinet components.
- **Electrostatic discharge (ESD) grounding cable with attached wrist strap** - Use of the ESD wrist strap is required when working in and around the director card cage.

- **Maintenance terminal (desktop or notebook PC)** - The PC is required to configure director network addresses and acquire event log information through the maintenance port. The PC must have:
  - The Microsoft Windows 98, Windows 2000, Windows XP, or Millennium Edition operating system installed.
  - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit** - The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

---

## Director Management

The director is managed and controlled through a:

- Management server running a SAN management application that provides a central point of control for up to 48 directors or managed products.

The management server is delivered with a *server* and *client* SAN management application (SANavigator or EFCM) and the Intrepid 6140 Element Manager application installed. A customer-supplied PC or workstation (with *client* applications installed) communicates with the server through a corporate intranet.

- Customer-supplied PC platform with an Internet connection to the SANpilot interface on the director. Using this graphical user interface (GUI), operators can quickly view director status.

The interface allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor director status, port status, and performance. FRU status and system alert information are highly visible.

- Customer-supplied PC or UNIX-based platform with the *server* and *client* SANavigator and Intrepid 6140 Element Manager applications installed.
- Simple network management protocol (SNMP). An SNMP agent is implemented through the SAN management application that allows administrators on SNMP management workstations to

access director management information using any standard network management tool. Administrators can assign internet protocol (IP) addresses and corresponding community names for up to 12 SNMP workstations functioning as SNMP trap message recipients. Refer to the *McDATA SNMP Support Manual* (620-000131).

- Command line interface (CLI). The CLI allows you to access many SAN management functions while entering commands during a telnet session with the director. The primary purpose of the CLI is to automate management of a large number of directors using scripts. The CLI is not an interactive interface; no checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to the *McDATA Command Line Interface User Manual* (620-000134).



This chapter describes tasks to install, configure, and verify operation of the Intrepid 6140 Director, management server, and SANpilot interface. The director can be mounted in a McDATA FC-512 Fabriccenter equipment cabinet, in a standard 19-inch equipment rack, or on a table top.

## Factory Defaults

[Table 2-1](#) lists the defaults for the Intrepid 6140 Director.

**Table 2-1     Factory-Set Defaults (Intrepid 6140 Director)**

Item	Default
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
SANpilot interface user name (case sensitive)	Administrator
SANpilot interface password (case sensitive)	password
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Table 2-2 lists the defaults for the one rack unit (1U) high, rack-mount management server.

**Table 2-2 Factory-Set Defaults (Management Server)**

Item		Default
Liquid crystal display (LCD) front panel		9999
Windows 2000 operating system user name (case sensitive)		Administrator
Windows 2000 operating system password (case sensitive)		password
SAN management application user name (case sensitive)		Administrator
SAN management application password (case sensitive)		password
LAN 1 (public interface)	IP address	192.168.0.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0
LAN 2 (private interface)	IP address	10.1.1.1
	Subnet mask	255.0.0.0
	Gateway address	0.0.0.0



## Installation Options

**NOTE:** The screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The director is installed in one of the following configurations:

- Fabriccenter equipment cabinet - Up to three directors, a rack-mount management server, and an Ethernet hub are delivered (cabled and installed) in a McDATA equipment cabinet. Ethernet cabling, distance, and local area network (LAN) addressing issues must only be considered if multiple cabinets are daisy-chained.
- Customer-supplied equipment rack - One or more directors, an optional management server, and an optional Ethernet hub are delivered to the customer facility for installation in a customer-supplied equipment rack. Rack mount flanges and hardware are provided in the shipping container. Ethernet cabling, distance, and LAN addressing issues must be considered.
- Table or desktop - One or more directors, an optional management server, and an optional Ethernet hub are delivered and installed at the customer facility on a table or desktop. Ethernet cabling, distance, and local area network (LAN) addressing issues must be considered.

## Summary of Installation Tasks

[Table 2-3](#) summarizes installation tasks for the director, optional management server, and optional Ethernet hub. The table describes each task, states if the task is required or optional, and lists the page reference.

Table 2-3 Installation Task Summary

Task Number and Description	Required or Optional	Page
<i>Task 1: Verify Installation Requirements.</i>	Required.	<a href="#">2-8</a>
<i>Task 2: Install the Ethernet Hub.</i>	Optional - perform this task only if the hub is required to connect the director to the management server or to the Internet (SANpilot interface).	<a href="#">2-9</a>
<i>Task 3: Install the Director.</i>	Required.	<a href="#">2-12</a>
<i>Subtask A: Unpack and Inspect the Director</i>	Required - if not installed in equipment cabinet.	<a href="#">2-12</a>
<i>Subtask B: Rack-Mount Installation</i>	Required - if not installed in equipment cabinet.	<a href="#">2-13</a>
<i>Subtask C: Turn-on Director Power</i>	Required.	<a href="#">2-13</a>
<i>Task 4: Configure Director Network Information.</i>	Configure if connecting multiple directors (not in a Fabriccenter cabinet) or if connecting a director and management server to a public LAN.	<a href="#">2-15</a>
<i>Subtask A: Set Network Addresses (IP Address, Subnet mask, Gateway Address)</i>	Configure if connecting multiple directors (not in a Fabriccenter cabinet) or if connecting a director and management server to a public LAN.	<a href="#">2-15</a>
<i>Subtask B: LAN-Connect the Director.</i>	Configure if connecting multiple directors (not in a Fabriccenter cabinet) or if connecting a director and management server to a public LAN.	<a href="#">2-19</a>
<i>Task 5: Install the Management Server.</i>	Required if the management server is installed.	<a href="#">2-20</a>
<i>Task 6: Configure the Management Server.</i>	Required if the management server is installed.	<a href="#">2-22</a>
<i>Subtask A: Configure Password and Network Addresses.</i>	Required if the management server is installed.	<a href="#">2-22</a>
<i>Subtask B: Configure Management Server Information.</i>	Required if the management server is installed.	<a href="#">2-25</a>
<i>Subtask C: Configure Windows 2000 Users.</i>	Required if the management server is installed.	<a href="#">2-30</a>
<i>Subtask D: Set Management Server Date and Time.</i>	Required if the management server is installed.	<a href="#">2-36</a>
<i>Subtask E: Configure the Call-Home Feature.</i>	Optional - configure if specified by the customer and a telephone connection is provided.	<a href="#">2-38</a>
<i>Subtask F: Record or Verify Management Server Restore Information</i>	Required if the management server is installed.	<a href="#">2-39</a>
<i>Task 7: Configure Director to the SAN Management Application</i>	Required if the management server is installed.	<a href="#">2-39</a>

Table 2-3 Installation Task Summary (*continued*)

Task Number and Description	Required or Optional	Page
<i>Subtask A: Assign User Names and Passwords to SAN Management Application.</i>	Required if the management server is installed.	<a href="#">2-39</a>
<i>Subtask B: Identify the Director to the SAN Management Application.</i>	Required if the management server is installed.	<a href="#">2-42</a>
<i>Subtask C: Verify Director-to-SAN Management Application Communication</i>	Required if the management server is installed.	<a href="#">2-43</a>
<i>Subtask D: Configure Feature Key.</i>	Configure if a feature key is ordered by the customer.	<a href="#">2-45</a>
<i>Subtask E: Configure Open Systems Management Server (OSMS) or FICON Management Server (FMS).</i>	Optional - configure for host control of the director (open systems or FICON).	<a href="#">2-46</a>
<i>Task 8: Configure the Director at the Element Manager Application.</i>	Required if the Element Manager application is installed.	<a href="#">2-49</a>
<i>Subtask A: Set Director Date and Time</i>	Required if the Element Manager application is installed.	<a href="#">2-50</a>
<i>Subtask B: Configure Director Identification</i>	Required if the Element Manager application is installed.	<a href="#">2-51</a>
<i>Subtask C: Configure Director Management Style</i>	Required if the Element Manager application is installed.	<a href="#">2-52</a>
<i>Subtask D: Configure Director Parameters</i>	Required if the Element Manager application is installed.	<a href="#">2-53</a>
<i>Subtask E: Configure Fabric Parameters</i>	Required if the Element Manager application is installed.	<a href="#">2-55</a>
<i>Subtask F: Configure Preferred Paths</i>	Required if the Element Manager application is installed.	<a href="#">2-57</a>
<i>Subtask G: Configure Switch Binding</i>	Required if the Element Manager application is installed.	<a href="#">2-59</a>
<i>Subtask H: Configure Director Ports</i>	Required if the Element Manager application is installed.	<a href="#">2-63</a>
<i>Subtask I: Configure SNMP Trap Message Recipients</i>	Required if the Element Manager application is installed.	<a href="#">2-66</a>
<i>Subtask J: Configure Threshold Alerts</i>	Required if the Element Manager application is installed.	<a href="#">2-67</a>
<i>Subtask K: Configure OpenTrunking</i>	Required if the Element Manager application is installed.	<a href="#">2-71</a>

Table 2-3 Installation Task Summary (*continued*)

Task Number and Description	Required or Optional	Page
<i>Subtask L: Enable SANpilot Interface and Telnet Access</i>	Optional - configure for SANpilot interface.	<a href="#">2-73</a>
<i>Subtask M: Configure, Enable, and Test E-mail Notification</i>	Optional - configure for e-mail notification.	<a href="#">2-73</a>
<i>Subtask N: Configure and Enable Ethernet Events</i>		<a href="#">2-75</a>
<i>Subtask O: Configure, Enable, and Test Call-Home Notification</i>	Optional - configure for call-home notification.	<a href="#">2-76</a>
<a href="#">Task 9: Configure SANtegrity Authentication (Optional)</a>	Optional - configure SANtegrity security features.	<a href="#">2-77</a>
<i>Task 11: Configure the Director at the SANpilot Interface.</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-80</a>
<i>Subtask A: Connect Director to Internet or Ethernet LAN Segment</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-82</a>
<i>Subtask B: Open the SANpilot Interface</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-82</a>
<i>Subtask C: Configure Director Ports</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-84</a>
<i>Subtask D: Configure BB Credit</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-85</a>
<i>Subtask E: Configure Director Identification</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-84</a>
<i>Subtask F: Configure Date and Time</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-87</a>
<i>Subtask G: Configure Operating Parameters</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-88</a>
<i>Subtask H: Configure Fabric Parameters</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-91</a>
<i>Subtask I: Configure Network Information</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-93</a>
<i>Subtask J: Configure SNMP</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-95</a>
<i>Subtask K: Enable or Disable the CLI or SSH</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-97</a>

Table 2-3 Installation Task Summary (*continued*)

Task Number and Description	Required or Optional	Page
<i>Subtask L: Enable or Disable OSMS and Host Control</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-98</a>
<i>Subtask M: Change User Passwords</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-99</a>
<i>Subtask N: Configure Port Binding</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-100</a>
<i>Subtask O: Configure Switch Binding</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-101</a>
<i>Subtask P: Configure Fabric Binding</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-106</a>
<i>Subtask Q: Enable or Disable Enterprise Fabric Mode</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-107</a>
<i>Subtask R: Configure OpenTrunking</i>	Required if the director is managed through the SANpilot interface.	<a href="#">2-108</a>
<i>Subtask S: Install Feature Keys</i>	Optional - configure if a feature key is ordered by the customer.	<a href="#">2-111</a>
<i>Task 12: Cable Fibre Channel Ports.</i>	Required.	<a href="#">2-113</a>
<i>Task 13: Configure Zoning.</i>	Perform this task to configure zoning.	<a href="#">2-113</a>
<i>Task 14: Connect the Director to a Fabric Element.</i>	Perform this task to connect the director to a fabric.	<a href="#">2-118</a>
<i>Task 15: Register with the McDATA File Center.</i>	Required.	<a href="#">2-120</a>

## Task 1: Verify Installation Requirements

Verify the following requirements are met prior to director installation. Ensure:

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to the *McDATA Products in a SAN Environment Planning Manual* (620-000124).
- Fabric and device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *McDATA Products in a SAN Environment Planning Manual* (620-000124).
- Support is available for one of the following director management methods:
  - A PC and LAN segment connectivity to the management server to support director management through the SAN management (SANavigator or EFCM) and Element Manager applications.
  - A PC and Internet connectivity to support director management through the SANpilot interface, or
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables (multimode or singlemode) are delivered and available. Ensure the cables are the correct length with the required connectors.
- A customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a corporate or dedicated LAN.

## Task 2: Install the Ethernet Hub

This task provides the instructions to unpack and inspect one or more Ethernet hubs and install the hubs on a desktop or in a rack-mount configuration.

**NOTE:** If the hub is delivered (with the director and management server) as part of a McDATA FC-512 Fabriccenter equipment cabinet, go to [Task 7: Configure Director to the SAN Management Application](#) on page 2-39.

Unpack and inspect the Ethernet hub(s).

1. Inspect shipping container(s) for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack shipping container(s) and inspect each item for damage. Ensure the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, contact the McDATA Solution Center.

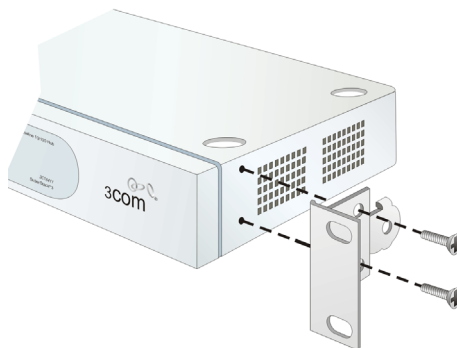
**Phone:** (800) 752-4572 or (720) 566-3910

**Fax:** (720) 566-3851

**E-mail:** [support@mcddata.com](mailto:support@mcddata.com)

Perform the following steps to install and configure up to three Ethernet hubs in a Fabriccenter equipment cabinet or a customer-supplied 19-inch equipment rack. A pointed instrument (pencil tip or bent paper clip), #2 Phillips screwdriver, and 1/8-inch Allen wrench are required.

1. Secure one mounting bracket to each side of the first hub ([Figure 2-1](#)). Use the two brackets and four pan-head Phillips screws (8/32 x 0.5-inch) provided.

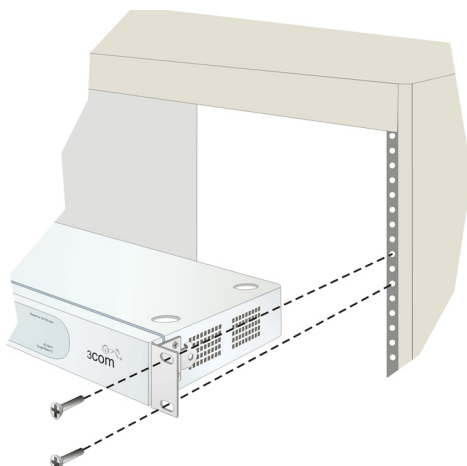


**Figure 2-1 Mounting Bracket Installation (Ethernet Hub)**

2. Position the first hub in the equipment rack as directed by the customer. Align screw holes in the mounting brackets with screw holes in the rack-mount standards.

**NOTE:** The hub is 1.75 inches, or one rack unit (1U) high.

3. Secure both sides of the hub to the rack-mount standards ([Figure 2-2](#)). Use the 1/8-inch Allen wrench and four Allen-head mounting screws (10/32 x 0.5-inch) provided.



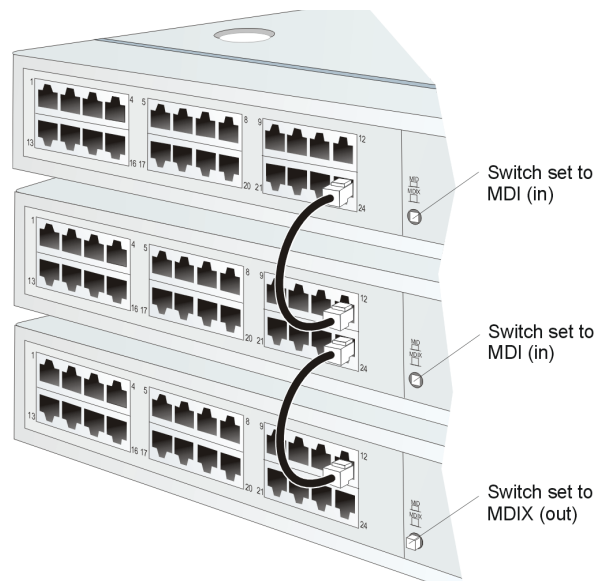
**Figure 2-2 Rack Installation (Ethernet Hub)**

4. Repeat [step 1](#) through [step 3](#) for the second and third hubs.



5. To daisy-chain (connect) the hubs:
  - a. To connect the top and middle hubs in the stack, connect an RJ-45 patch cable to port 24 of the top hub, then connect the cable to port 12 of the middle hub.
  - b. To connect the bottom and middle hubs in the stack, connect a second RJ-45 patch cable to port 24 of the middle hub, then connect the cable to port 12 of the bottom hub.
  - c. Using a pencil or other pointed instrument, set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI (in)**. Set the MDI switch on the bottom hub to **MDIX (out)**. The configuration is shown in [Figure 2-3](#).

**NOTE:** To connect two hubs, use [step a](#) and [step c](#) (top and middle hub instructions only).



**Figure 2-3 Patch Cable and MDI Selector Configuration**

6. Connect an AC power cord to the receptacle at the rear of each hub and to a rack power strip. Power for each hub switches on when the hub (and equipment rack) are connected to facility AC power.

---

**NOTE:** Ensure each hub is connected to a separate rack power strip.

---

7. Inspect the front panel of each hub. Ensure each green **Power** LED illuminates.

---

## Task 3: Install the Director



### CAUTION

---

**Use safe lifting practices when moving the product.**

---

This task provides instructions to unpack the director, install the director in a rack-mount configuration, and perform initial configuration functions.

---

**NOTE:** If the director is delivered as part of a FC-512 Fabriccenter equipment cabinet, refer to the *McDATA FC-512 Fabriccenter Equipment Cabinet Installation and Service Manual* (620-000100) for unpacking and installation instructions. Turn-on director power ([Subtask C: Turn-on Director Power](#) on page 2-13) and go to [Task 5: Install the Management Server](#) on page 2-20.

---

---

### Subtask A: Unpack and Inspect the Director

Unpack and inspect the director.

1. Inspect the shipping containers for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack the shipping containers and inspect each item for damage. Ensure the items match the items listed on the bill of materials (BOM).
3. If any items are damaged or missing, contact the McDATA Solution Center.

**Phone:** (800) 752-4572 or (720) 566-3910

**Fax:** (720) 566-3851

**E-mail:** [support@mcddata.com](mailto:support@mcddata.com)

## Subtask B: Rack-Mount Installation



### CAUTION

**Use safe lifting practices when moving the product.**

Perform the following steps to install the director in a customer-supplied equipment rack. A #2 Phillips screwdriver is required.

1. Locate the rack-mount position as directed by the customer. The director is 20 inches (12 U) high.
2. Verify all FRUs, including the SFP and XFP optical transceivers, logic cards, fans, and power supplies are installed as ordered.
3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and verify all parts are delivered.
4. Using installation instructions delivered with the rack-mount kit and a #2 Phillips screwdriver, install the director in the equipment cabinet.

## Subtask C: Turn-on Director Power



### DANGER

***Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.***

1. Connect the U.S. AC power cords to the right (PS0) and left (PS1) receptacles at the rear of the director ([Figure 2-4](#)).
2. Connect the remaining ends of the AC power cords to separate (for redundancy) rack power strips.

**NOTE:** The director does not have a power switch. Therefore the director powers on when its power cords are connected to facility or rack power.



**Figure 2-4 AC Power Connections (Director)**

3. Connect the equipment rack power cords to separate (for redundancy) facility power sources that provide single-phase, 180 to 264 VAC voltage.
4. Power on the rack power strips.
5. Inspect the front panel of each rack-mounted Ethernet hub. Ensure each green **Power** LED illuminates.
6. The director powers on and performs POSTs. During POSTs:
  - Amber LEDs on both CTP cards and all port cards illuminate momentarily.
  - The green LED on each CTP card (active and backup) and each port card illuminate as the card is tested.
  - Green LEDs associated with Fibre Channel ports sequentially illuminate as the ports are tested.
7. After successful POST completion
  - Bezel: **POWER** LED green
  - Active CTP card: LED green
  - Power supplies: **PWR OK** LEDs green
8. If a POST error or other malfunction occurs, go to [Chapter 3, Maintenance Analysis Procedures \(MAPS\)](#) to isolate the problem.

## Task 4: Configure Director Network Information

The director is delivered with the following default network addresses ([Table 2-4](#)):

**Table 2-4 Factory-Set Defaults (Intrepid 6140 Director)**

Item	Default
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
SANpilot interface user name (case sensitive)	Administrator
SANpilot interface password (case sensitive)	password
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Verify the type of LAN installation with the customer network administrator.

- If one director is installed on a dedicated LAN, network addresses do not require change. Go to [Task 5: Install the Management Server](#) on page 2-20 or to [Task 11: Configure the Director at the SANpilot Interface](#) on page 2-80
- If multiple directors are installed or a public LAN segment is used, network addresses must be changed to conform to the customer LAN addressing plan. Continue to [Subtask A: Set Network Addresses \(IP Address, Subnet mask, Gateway Address\)](#) following.

### Subtask A: Set Network Addresses (IP Address, Subnet mask, Gateway Address)

Perform the following steps to verify or change a director IP address, subnet mask, or gateway address.

1. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a Phillips screwdriver may be required). Connect the 9-pin end of the RS-232 modem cable to the port.

2. Connect the other cable end to a 9-pin communication port (COM1 or COM2) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays. If required, refer to operating instructions shipped with the PC.
4. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

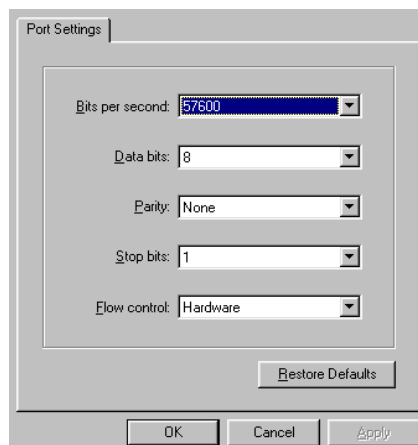
**NOTE:** The following steps describe changing network addresses using HyperTerminal serial communication software.

5. At the *Windows Workstation* menu, sequentially select *Programs*, *Accessories*, *Communications*, and *HyperTerminal*. The *Connection Description* dialog box displays (Figure 2-5).



**Figure 2-5** Connection Description Dialog Box

6. Type **Intrepid 6140** in the *Name* field and click *OK*. The *Connect To* dialog box displays.
7. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the director), and click *OK*. The *COMn* dialog box (Figure 2-6) displays (where *n* is 1 or 2).



**Figure 2-6 COMn Properties Dialog Box**

8. Configure the *Port Settings* parameters.

- Bits per second - **115200**.
- Data bits - **8**.
- Parity - **None**.
- Stop bits - **1**.
- Flow control - **Hardware** or **None**.

When the parameters are set, click *OK*. The *Intrepid 6140 - HyperTerminal* dialog box displays.

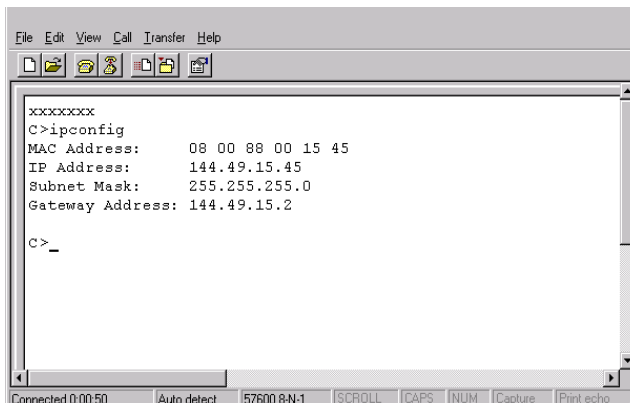
9. At the **>** prompt, type the user-level password (the default is **password**) and press **Enter**. The password is case sensitive. The *Intrepid 6140 - HyperTerminal* dialog box displays with software and hardware version information for the director, and a **C>** prompt at the bottom of the window.
10. At the **C>** prompt, type **ipconfig** and press **Enter**. The *Intrepid 6140 - HyperTerminal* dialog box (Figure 2-7) displays with configuration information listed.
  - *MAC Address*.
  - *IP Address* (default is **10.1.1.10**).
  - *Subnet Mask* (default is **255.0.0.0**).
  - *Gateway Address* (default is **0.0.0.0**).

— *Auto Negotiate*.

— *Speed*.

— *Duplex*.

Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.



**Figure 2-7** HyperTerminal Dialog Box

11. Change the IP address, subnet mask, and gateway address as directed by the customer network administrator. To change director network addresses, type the following at the **C>** prompt and press **Enter**.

**ipconfig xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz**

Where:

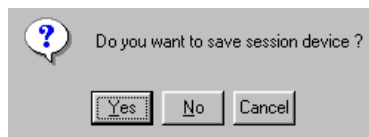
- The IP address is **xxx.xxx.xxx.xxx**
- The subnet mask is **yyy.yyy.yyy.yyy**
- The gateway address is **zzz.zzz.zzz.zzz**

Where the octets **xxx**, **yyy**, and **zzz** are decimals from zero through 255.

12. The message **Request completed OK** displays at the bottom of the *Intrepid 6140 - HyperTerminal* dialog box after the network addresses are configured.
13. Select *Exit* from the *File* pull-down menu to close the HyperTerminal application. A HyperTerminal message box appears.



14. Click *Yes*. A second HyperTerminal message box appears ([Figure 2-8](#)).



**Figure 2-8** HyperTerminal Dialog Box

15. Click *No* to exit and close the HyperTerminal application.
16. Power off the maintenance terminal:
17. Disconnect the RS-232 null modem cable from the director and the maintenance terminal. Replace the protective cap over the maintenance port.
18. IML the director ([IML the Director \(CTP Front Panel\)](#) on page 4-53).

---

## Subtask B: LAN-Connect the Director

To connect the director to the Ethernet LAN segment:

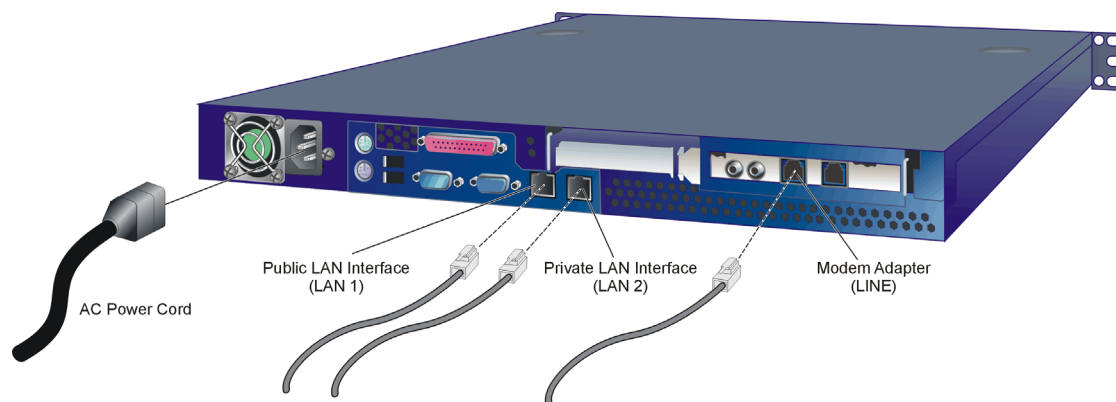
1. Connect one end of an Ethernet patch cable (two cables supplied with the director) to the RJ-45 connector on each CTP card.
2. Connect the remaining end of each Ethernet cable to the LAN.
  - If the director is to be installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer network administrator.
  - If the director is to be installed on the McDATA-qualified Ethernet hub, connect the cable to any available hub port.
3. Perform one of the following steps:
  - If the director is delivered separately from the management server, go to [Task 5: Install the Management Server](#) following.
  - If the director is managed through the SANpilot interface, attach the Ethernet LAN segment to an Internet connection and go to [Task 11: Configure the Director at the SANpilot Interface](#) on page 2-80.

## Task 5: Install the Management Server

The management server is a 1U high, rack-mount unit with the SAN management (SANavigator or EFCM) and Intrepid 6140 Element Manager applications installed. This task provides instructions to unpack, install, and configure the management server.

Unpack, inspect, and install the management server.

1. Inspect the shipping container for damage caused during transit. If a container is damaged, ensure a representative from the freight carrier is present when the container is opened.
2. Unpack the shipping container and inspect each item for damage. Ensure the packaged items correspond to the items on the bill of materials.
3. If any items are damaged or missing, customers should call the toll-free telephone number printed on the service label attached to the bottom of the server.
4. Open the rack-mount kit and inspect the contents. Refer to the bill of materials and verify all parts are delivered.
5. Install the management server in the equipment cabinet (*1U Server Rack-Mount Kit Installation Instructions*, 958-000310).
6. Connect the management server to the customer-supplied Ethernet LAN segment or McDATA-qualified Ethernet hub (private LAN interface). To connect the server:
  - a. Connect one end of the Ethernet patch cable (supplied with the management server) to the right RJ-45 adapter (**LAN 2**) at the rear of the server ([Figure 2-9](#)).



**Figure 2-9 Management Server Connections**

- b. Connect the remaining end of the Ethernet cable to the LAN.
    - If the server is installed on a customer-supplied LAN segment, connect the cable to the LAN as directed by the customer network administrator.
    - If the server is installed on the McDATA-qualified Ethernet hub, connect the cable to any available hub port.
7. If required, connect the management server to the customer corporate intranet (public LAN interface). To connect the server:
  - a. Connect one end of a customer-supplied Ethernet patch cable to the left RJ-45 adapter (**LAN 1**) at the rear of the server ([Figure 2-9](#)).
  - b. Connect the remaining end of the Ethernet cable to the corporate intranet as directed by the customer network administrator.
8. Connect the 20-foot phone cord to the left RJ-11 adapter (**LINE**) at the rear of the server and to a facility telephone connection ([Figure 2-9](#)).
9. Connect the AC power cord to the server and to a facility power source or rack power strip that provides single-phase, 90 to 264 VAC current ([Figure 2-9](#)).
10. When the power cord is connected, the management server powers on and performs power-on self-tests (POSTs). During POSTs:

- The green liquid crystal display (LCD) panel illuminates.
- The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
- The server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
- 11. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- 12. If a POST error or other malfunction occurs, go to [Chapter 3, Maintenance Analysis Procedures \(MAPS\)](#) to isolate the problem.
- 13. Press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
- 14. Insert a blank rewritable CD into the CD-RW drive and close the LCD panel.

---

## Task 6: Configure the Management Server

---

### Subtask A: Configure Password and Network Addresses

Verify the type of LAN installation with the customer network administrator.

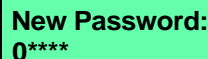
- If the management server or Fabriccenter equipment cabinet is installed on a dedicated LAN, network information does not require change. Change the default password for the server LCD panel (if required by the customer), then go to [Subtask B: Configure Management Server Information](#) on page 2-25.
- If the management server or Fabriccenter equipment cabinet is installed on a public LAN segment, the default password for the server LCD panel and the transmission control protocol internet protocol (TCP/IP) network information (IP address and subnet mask) must be changed to conform to the customer LAN addressing plan.

**NOTE:** At some customer installations, TCP/IP addresses for the management server may be allocated automatically using dynamic host configuration protocol (DHCP).

## Configure Password

To configure a new LCD panel password:

1. At the management server LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the **Input Password** panel.
2. Use the arrow keys to input the default password (**9999**) and press **ENTER**. The **LAN 1 Setting??** message appears.
3. Press the down-arrow button several times until the **Change Password?** option appears and press **ENTER**. The following message appears ([Figure 2-10](#)).



New Password:  
0\*\*\*\*

**Figure 2-10** LCD Panel (New Password)

4. Use the arrow keys to input a new 4-digit numeric password and press **ENTER**. The **Save Change** panel appears.
5. Press **ENTER**. The panel returns to the **LAN 1 Setting??** message and the password changes.

## Configure Private LAN Addresses

To configure TCP/IP network information for the private LAN connection (LAN 2):

1. At the management server LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the **Input Password** panel.
2. Use the arrow keys to input the default or changed password and press **ENTER**. The **LAN 1 Setting??** message appears.
3. Press the down-arrow button. The **LAN 2 Setting??** message appears. Press **ENTER** and the following message appears (Figure 2-11).



**Input IP:**  
**010.001.001.001**

**Figure 2-11 LCD Panel (LAN 2 IP Address)**

4. Use the arrow keys to input a new IP address and press **ENTER**. The **Save Change** panel appears.
5. Press **ENTER**. The LAN 2 IP address changes and the following message appears (Figure 2-12).



**Input Netmask:**  
**255.000.000.000**

**Figure 2-12 LCD Panel (LAN 2 Subnet Mask)**

6. Use the arrow keys to input a new subnet mask and press **ENTER**. The **Save Change** panel appears.
7. Press **ENTER**. The panel returns to the **LAN 1 Setting??** message and the LAN 2 subnet mask changes.
8. Record the private LAN IP address and subnet mask.

## Configure Public LAN Addresses

To configure TCP/IP network information for the public LAN connection (LAN 1):

1. At the management server LCD panel, press **ENTER**. The **Welcome!!** or operational information message changes to the **Input Password** panel .
2. Use the arrow keys to input the default or changed password and press **ENTER**. The **LAN 1 Setting??** message appears.
3. Press **ENTER** and the following message appears ([Figure 2-13](#)).

A green rectangular LCD panel with a black border. The text "Input IP:" is on the first line, and "192.168.000.001" is on the second line, both in black font.

**Input IP:**  
**192.168.000.001**

**Figure 2-13 LCD Panel (LAN 1 IP Address)**

4. Use the arrow keys to input a new IP address and press **ENTER**. The **Save Change** panel appears.
5. Press **ENTER**. The LAN 1 IP address changes and the following message appears ([Figure 2-14](#)).

A green rectangular LCD panel with a black border. The text "Input Netmask:" is on the first line, and "255.000.000.000" is on the second line, both in black font.

**Input Netmask:**  
**255.000.000.000**

**Figure 2-14 LCD Panel (LAN 1 Subnet Mask)**

6. Use the arrow keys to input a new subnet mask and press **ENTER**. The **Save Change** panel appears.
7. Press **ENTER**. A **Wait a moment!** message appears, the panel returns to the **LAN 1 Setting??** message, and the LAN 1 subnet mask changes.
8. Record the public LAN IP address and subnet mask.

---

## Subtask B: Configure Management Server Information

Configure the computer name and workgroup name for the management server. Configure these parameters from the server Windows 2000 operating system, using a LAN-attached PC with standard web browser.

If required, change the management server gateway addresses and domain name system (DNS) server IP addresses to conform to the

customer LAN addressing plan. The gateway addresses are the addresses of the local router for the corporate intranet.

## Access the Management Server Desktop

To login and access the management server desktop:

1. Ensure the management server and a PC are connected through an Ethernet LAN segment. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
2. At the PC browser, enter the LAN 2 IP address of the management server, followed by :5800, as the Internet uniform resource locator (URL). Entered the URL in the following format:

**http://xxx.xxx.xxx.xxx:5800**

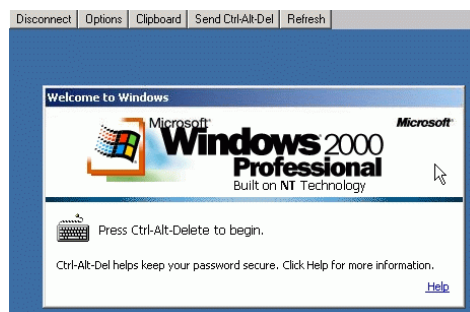
Where *xxx.xxx.xxx.xxx* is the default IP address of **10.1.1.1** or the IP address configured while performing *Subtask A: Configure Password and Network Addresses* on page 2-22. The VNC Authentication screen displays.

3. Type the default password and click OK. The *Welcome to Windows* dialog box displays (Figure 2-15).

---

**NOTE:** The default TightVNC viewer password is **password**.

---



**Figure 2-15** Welcome to Windows Dialog Box

4. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays (Figure 2-16).

---

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action logs the user on to the PC, not the management server.

---





Figure 2-16 Log On to Windows Dialog Box

5. Type the default Windows 2000 user name and password and click OK. The management server Windows 2000 desktop opens and the *EFCM Log In* or *SANavigator Log In* dialog box displays (Figure 2-17).

**NOTE:** The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

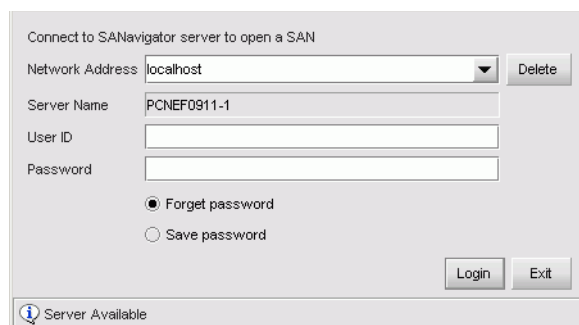
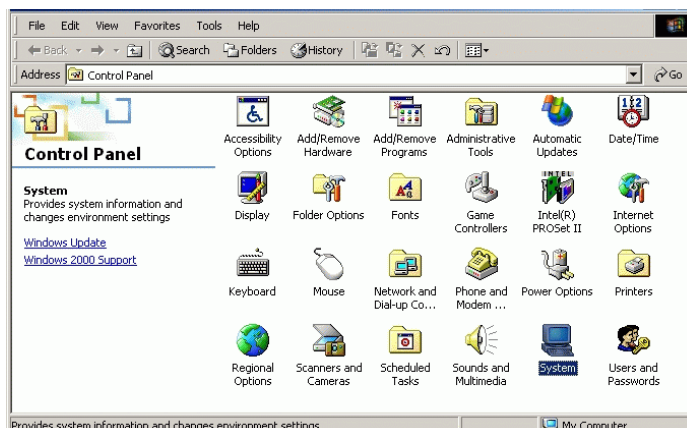


Figure 2-17 EFCM Log In or SANavigator Log In Dialog Box

## Configure Management Server Names

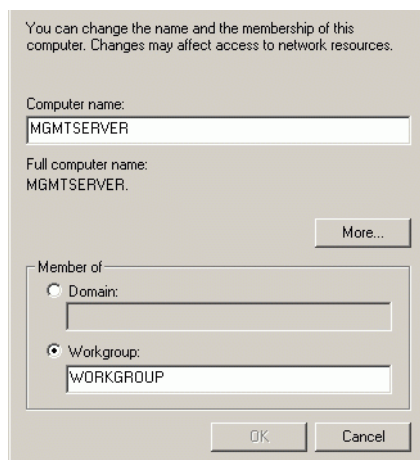
To configure the management server name and workgroup name:

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-18).



**Figure 2-18 Control Panel Window**

2. Click the *Network Identification* tab. The *System Properties* dialog box displays with the *Network Identification* tab selected.
3. Click *Properties*. The *Identification Changes* dialog box displays (Figure 2-19).



**Figure 2-19 Identification Changes Dialog Box**

4. At the *Computer Name* field, change the name to **MGMTSERVER**, at the *Workgroup* field, change the name to **WORKGROUP**, then click **OK**. The dialog box closes.

5. Record the computer and workgroup names.
6. At the *System Properties* dialog box, click *OK* to close the dialog box and return to the *Control Panel* window.
7. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

## Configure Gateway and DNS Server Addresses

To configure gateway addresses and DNS server IP addresses for the private LAN connection (LAN 2) and optional public LAN connection (LAN 1):

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-18).
2. Double-click the *Network and Dial-up Connections* icon. The *Network and Dial-up Connections* window displays.
3. To configure addresses for the private LAN connection (LAN 2), double-click the *Local Area Connection 2* icon. The *Local Area Connection 2 Properties* dialog box displays.
4. Click *Properties*. The *Local Area Connection 2 Properties* dialog box displays.
5. Double-click the *Internet Protocol (TCP/IP)* entry. The *Internet Protocol (TCP/IP) Properties* dialog box displays (Figure 2-20).

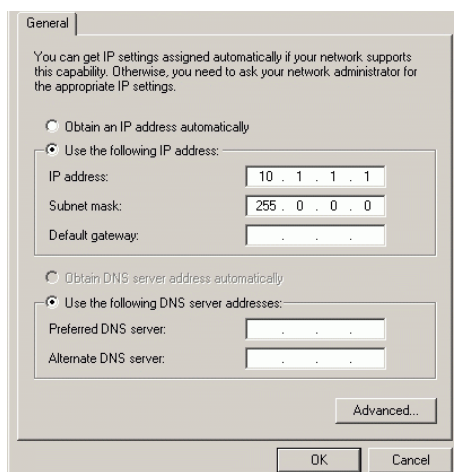


Figure 2-20 Internet Protocol (TCP/IP) Properties Dialog Box

6. The *Use the following IP address* radio button is enabled and the *IP address* and *Subnet mask* fields display network information configured while performing [Subtask A: Configure Password and Network Addresses](#) on page 2-22.
7. At the *Default gateway* field, enter the gateway address obtained from the customer network administrator.
8. Select (enable) the *Use the following DNS server addresses* radio button. At the *Preferred DNS server* field, enter the DNS server IP address obtained from the customer network administrator, then click OK to apply the changes and close the dialog box.
9. Click OK to close the *Local Area Connection 2 Properties* dialog box.
10. Record the changed gateway and DNS server addresses.
11. To optionally configure addresses for the public LAN connection (LAN 1), double-click the *Local Area Connection 1* icon and repeat [step 3](#) through [step 10](#).
12. Click close (X) at the upper right corner of the *Network and Dial-up Connections* window to return to the Windows 2000 desktop.
13. Reboot the management server:
  - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut down*. The *Shut Down Windows* dialog box appears.
  - b. At the *Shut Down Windows* dialog box, select the *Restart* option and click OK to reboot the server.
  - c. Perform [Access the Management Server Desktop](#) on page 2-26.

---

### Subtask C: Configure Windows 2000 Users

Configure password access for all authorized Windows 2000 users of the management server. It is also recommended to change the default administrator password. To configure users:

1. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Settings*, then *Control Panel*. The *Control Panel* window displays ([Figure 2-18](#)).
2. Double-click the *Users and Passwords* icon. The *Users and Passwords* dialog box displays ([Figure 2-21](#)).

3. The *Guest* user name is a built-in account in the Windows 2000 operating system and cannot be deleted. The *srvacc* account is for field service users and must not be modified or deleted.

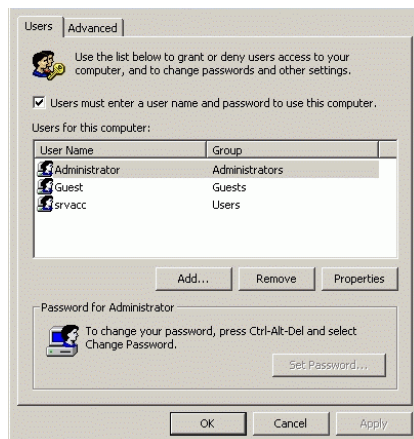


Figure 2-21 Users and Passwords Dialog Box

## Change Default Administrator Password

To change the administrator password from the default (**password**) to a customer-specified password:

1. Click the **Send Ctrl-Alt-Del** button at the top of the window surrounding the *Users and Passwords* dialog box. The *Windows Security* dialog box displays (Figure 2-22).

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action controls the PC, not the rack-mount management server.



**Figure 2-22 Windows Security Dialog Box**

2. Click *Change Password*. The *Change Password* dialog box displays (Figure 2-23).



**Figure 2-23 Change Password Dialog Box**

3. At the *Old Password* field, type the old password. At the *New Password* and *Confirm New Password* fields, type the new password.

---

**NOTE:** The *New Password* and *Confirm New Password* fields are case-sensitive.

---

4. Click *OK*. The default administrator password changes and the *Change Password* dialog box closes.
5. Click *Cancel* at the *Windows Security* dialog box to return to the *Users and Passwords* dialog box.

## Add a New User

To set up a new Windows 2000 user:

1. At the *Users and Passwords* dialog box, click *Add*. The first window of the *Add New User* wizard displays (Figure 2-24).

The screenshot shows the first window of the 'Add New User' wizard. On the left is a blue vertical bar with a white icon of a person and a key. The main area is light gray and contains the text 'Enter the basic information for the new user.' Below this are three text input fields labeled 'User name:', 'Full name:', and 'Description:'. Below the fields is the text 'To continue, click Next.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

**Figure 2-24 Add New User Wizard (First Window)**

2. Type the new user information in the *User name*, *Full name*, and *Description* fields, then click *Next*. The second window of the *Add New User* wizard displays (Figure 2-25).

The screenshot shows the second window of the 'Add New User' wizard. On the left is a blue vertical bar with a white icon of a person and a key. The main area is light gray and contains the text 'Type and confirm a password for this user.' Below this are two text input fields labeled 'Password:' and 'Confirm password:'. Below the fields is the text 'To continue, click Next.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

**Figure 2-25 Add New User Wizard (Second Window)**

3. Type the new user password in the *Password* and *Confirm password* fields, then click *Next*. The third window of the *Add New User* wizard displays (Figure 2-26).



**Figure 2-26 Add New User Wizard (Third Window)**

4. Based on the level of access to be granted, select the *Standard user*, *Restricted user*, or *Other* radio button. If the *Other* radio button is selected, choose the type of access from the adjacent list box.
5. Click *Finish*. The new user information is added and the wizard closes. Record the user information.
6. If no other users are to be added, click *OK* to close the *Users and Passwords* dialog box.
7. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

## Change User Properties

To change user properties:

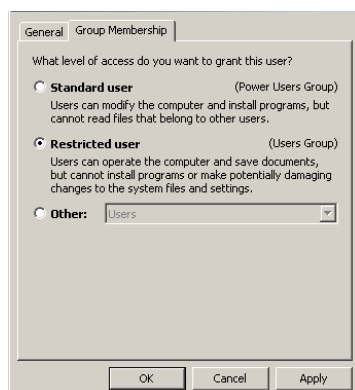
1. At the *Users and Passwords* dialog box, highlight the user (**srvacc**, for example) at the *Users for this computer* field and click *Properties*. The **MGMTSERVER\srvacc Properties** dialog box displays with the *General* tab selected ([Figure 2-27](#)).





**Figure 2-27** MGMTSERVER\srvacc Properties Dialog Box (General Tab)

2. Type the new user information in the *User name*, *Full name*, and *Description* fields, then click the *Group Membership* tab. The MGMTSERVER\srvacc Properties dialog box displays with the *Group Membership* tab selected (Figure 2-28).



**Figure 2-28** MGMTSERVER\srvacc Properties Dialog Box (Group Membership Tab)

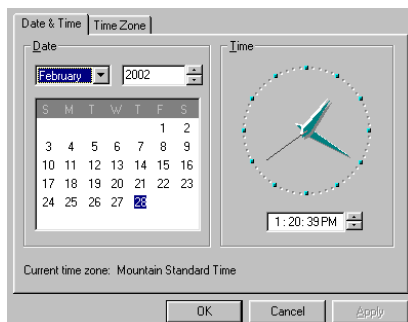
3. Based on the level of access to be changed, select the *Standard user*, *Restricted user*, or *Other* radio button. If the *Other* radio button is selected, choose the type of access from the adjacent list box.
4. Click OK. The new user information is added and the MGMTSERVER\srvacc Properties dialog box closes. Record the user information.

5. If no other users are to be changed, click *OK* to close the *Users and Passwords* dialog box.
6. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

### Subtask D: Set Management Server Date and Time

The SAN management application audit and event logs are time-stamped with the date and time from the management server. The director system clock is synchronized with the date and time of the management server by default. To set the server date and time:

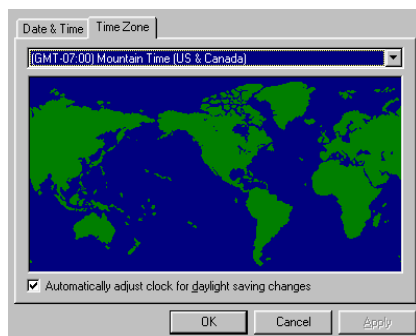
1. At the Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Settings*, then *Control Panel*. The *Control Panel* window displays (Figure 2-18).
2. Double-click the *Date/Time* icon. The *Date/Time Properties* dialog box displays with the *Date & Time* page open (Figure 2-29).



**Figure 2-29 Date/Time Properties Dialog Box (Date & Time Tab)**

**NOTE:** The *Time Zone* field must be set before the *Date & Time* field.

3. Click the *Time Zone* tab. The *Date/Time Properties* dialog box displays with the *Time Zone* page open (Figure 2-30).



**Figure 2-30 Date/Time Properties Dialog Box (Time Zone Tab)**

4. To change the time zone:
  - a. Select the time zone from the drop-down list at the top of the dialog box.
  - b. If instructed by the customer system administrator, select the *Automatically adjust clock for daylight saving changes* check box.
  - c. Click *Apply*. Record time zone and daylight savings information.
5. Click the *Date & Time* tab. The *Date/Time Properties* dialog box displays with the *Date & Time* page open.
6. To change the date and time:
  - a. Select the month from the drop-down list under *Date*.
  - b. Click the up or down arrow adjacent to the year field and select the desired year.
  - c. Click the day on the calendar to select the desired date.
  - d. Click in the time field and enter the desired time, then click the adjacent up or down arrow and select *AM* or *PM*.
  - e. Click *Apply*. Record date and time information.
7. Click *OK* to close the *Date/Time Properties* dialog box.
8. Click close (X) at the upper right corner of the *Control Panel* window to return to the Windows 2000 desktop.

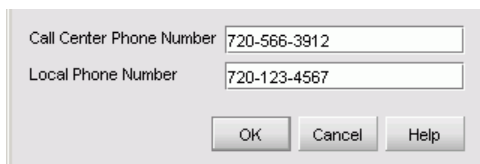
## Subtask E: Configure the Call-Home Feature

**NOTE:** The call-home feature may not be available if the EFC Manager application (EFCM Lite) is installed on a customer-supplied PC.

**NOTE:** These steps are valid *only* for an initial installation. Several dialog boxes appearing in this procedure are configured only once per installation.

To configure the call-home feature:

1. There are two jacks on the management server internal modem: one for the call-home connection (**LINE**), and the other for a telephone (**PHONE**). Ensure a telephone cable is routed and connected to the **LINE** jack at the rear of the management server.
2. At the Windows 2000 desktop, double-click the *Call-Home Configuration* icon. The *Call Home Configuration* dialog box displays (Figure 2-31).



**Figure 2-31** Call Home Configuration Dialog Box

3. At the *Call Center Phone Number* field, enter the telephone number for the McDATA Solution Center (**720-566-3912**). Include necessary information, such as the country code, area code, or any prefix required to access a telephone line outside the facility.
4. At the *Local Phone Number* field, enter the telephone number for access to the local server. Include necessary information such as the country code or area code.
5. Click **OK** to save the configured telephone numbers and close the dialog box.

---

## Subtask F: Record or Verify Management Server Restore Information

Windows 2000 configuration information must be recorded to restore the management server in case of hard drive failure. Ensure that the following management server configuration information is verified or recorded:

- Network configuration information.
  - LCD panel password.
  - Network addresses (IP address, subnet mask, gateway address, and DNS server IP address) for private LAN connection (LAN 2).
  - Network addresses (IP address, subnet mask, gateway address, and DNS server IP address) for public LAN connection (LAN 1).
  - Computer name.
- User passwords.
- Date and time information.
- Product ID number.

---

## Task 7: Configure Director to the SAN Management Application

Perform the following tasks to configure the director to the SAN management application (SANavigator or EFCM).

---

### Subtask A: Assign User Names and Passwords to SAN Management Application

Users must be configured for access to the SAN management application.

To assign user names and passwords:

1. At the *EFCM Log In* or *SANavigator Log In* dialog box (Figure 2-17), type the SAN management application default user name and password and select a server or IP address from the *Network Address* drop-down list.

**NOTE:** The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

- Click *Login*. The application opens and the EFCM or SANavigator main window appears (Figure 2-32).

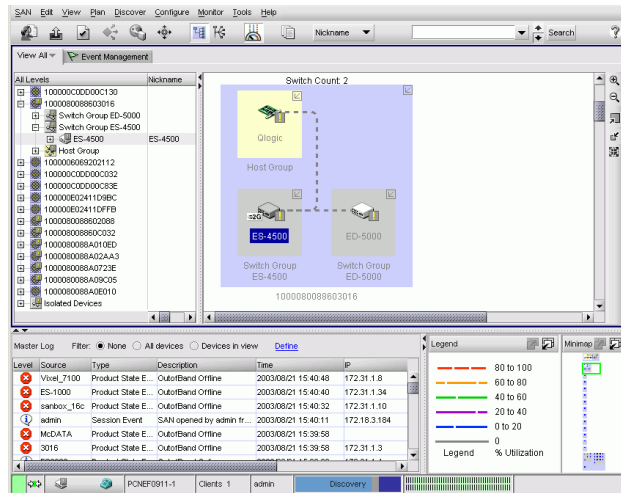


Figure 2-32 Main Window: Example (EFCM or SANavigator)

- Select *Users* from the SAN menu. The *EFCM Server* or *SANavigator Server Users* dialog box displays (Figure 2-33).

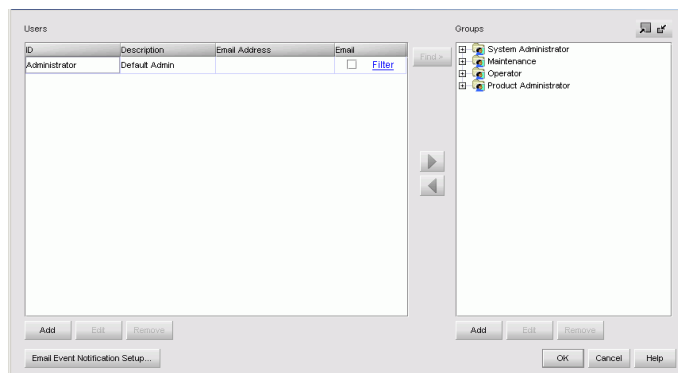
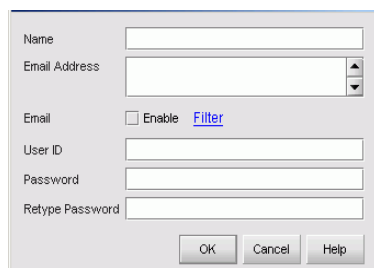


Figure 2-33 EFCM Server or SANavigator Users Dialog Box

- Click *Add*. The *Add User* dialog box displays (Figure 2-34).



The image shows a 'Add User Dialog Box' with the following fields and controls:

- Name:** A text input field.
- Email Address:** A text input field with a small up/down arrow on the right.
- Email:** A checkbox labeled 'Enable' followed by a blue hyperlink labeled 'Filter'.
- User ID:** A text input field.
- Password:** A text input field.
- Retype Password:** A text input field.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

**Figure 2-34 Add User Dialog Box**

5. Enter information in fields as directed by the customer:
  - **Name** - Click in this field and type a new user name up to 16 alphanumeric characters. Control characters and spaces are not valid. The user name is case-sensitive.
  - **Email Address** - Click in this field and type one or more new user e-mail addresses. Separate multiple addresses with a semicolon.
  - **User ID** - Click in this field and type a unique user ID for the new user.
  - **Password** - Click in this field and type a password up to 16 alphanumeric characters in length. Control characters and spaces are not valid. The password is case-sensitive.
  - **Retype Password** - To confirm the password is entered correctly, click in this field and enter the password exactly as in the *Password* field. If an incorrect keystroke is entered, use the **Backspace** key to delete individual letters or select (highlight) the entire entry and press **Delete**.
6. To enable e-mail notification for the new user, click the *Enable* check box.
7. To configure event types for which e-mail notification is sent, click the *Filter* link. The *Define Filter* dialog box displays. For instructions on defining event filters, refer to the *McDATA Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153), *McDATA Enterprise Fabric Connectivity Manager User Manual* (620-005001), or *SANavigator User Guide* (621-000013).
8. Click **OK** to accept the information and close the dialog box.
9. Repeat [step 4](#) through [step 8](#) to assign multiple user names and passwords.

10. When finished, click *OK* at the *EFCM Server* or *SANavigator Server Users* dialog box to return to the EFCM or SANavigator main window.

## Subtask B: Identify the Director to the SAN Management Application

To manage a new director, it must be identified to and discovered by the SAN management application. To identify the new director:

1. At the SAN management application (EFCM or SANavigator main window), select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 2-35).

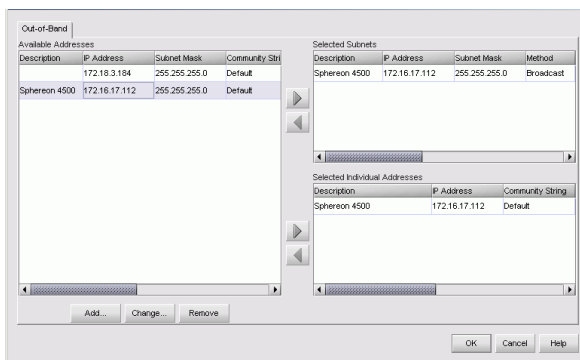
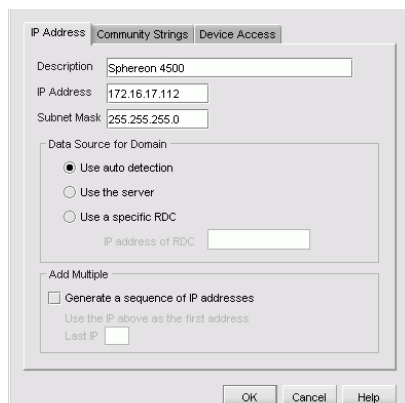


Figure 2-35 Discover Setup Dialog Box

2. Click *Add*. The *Domain Information* dialog box displays with the *IP Address* page open (Figure 2-36).





**Figure 2-36 Domain Information Dialog Box (IP Address Page)**

3. Type a director description in the *Description* field.
4. Type the director IP address in the *IP Address* field.
5. Type the director subnet mask in the *Subnet Mask* field.
6. At the *Data Source for Domain* area of the dialog box, select the *Use auto detection*, *Use the server*, or *Use a specific RDC* radio button.
7. Click *OK* to save the information, close the dialog box, and define the director to the SAN management application.
8. Repeat [step 2](#) through [step 7](#) for each new director or switch.
9. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.





### Subtask C: Verify Director-to-SAN Management Application Communication

Verify the communication between the director and management server (SAN management and Element Manager applications). To verify director-to-server communication:

1. At the SAN management application main window (physical map or product list), inspect the shape and color of the status symbol associated with the Intrepid 6140 Director icon. [Table 2-5](#) explains operational states and associated symbols.
2. Right-click the Intrepid 6140 product icon at the SAN management application physical map. A pop-up menu appears.

3. Select the *Element Manager* option from the pop-up menu. When the Element Manager application opens, the last view (tab) accessed by a user opens by default, such as the *Hardware View*.
4. Inspect director status at the *Hardware View* and perform one of the following:
  - If the director appears operational, go to [Subtask D: Configure Feature Key](#) on page 2-45.
  - If director operation appears degraded or a director failure is indicated, go to [Chapter 3, Maintenance Analysis Procedures \(MAPS\)](#) to isolate the problem.

**Table 2-5 Element Manager Alert Symbols, Messages, and Status**

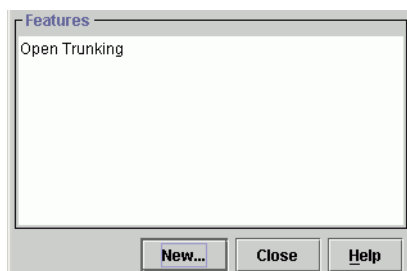
Symbol	Message	Description
	Fully operational	All components and installed ports are operational.
	Redundant failure	A redundant component has failed and the backup component has taken over.
	Minor failure	A failure has occurred that has decreased the director operational capability, but has not affected normal switching operations.
	Major failure	Power supplies have failed.
	Loading firmware	The system is busy loading new firmware, but the system is otherwise operational.
	Not operational	A critical failure has occurred that prevents the director from performing fundamental switching operations.
	<ul style="list-style-type: none"> <li>o Link time-out</li> <li>o Protocol mismatch</li> <li>o Never connected</li> </ul>	Director status is unknown. Occurs is network connection between the management server and the director is lost, or if a CTP card fails and there is no operational backup, or if there is no system power.

## Subtask D: Configure Feature Key

Perform this task to display features that have been installed or install features that are available for the director as customer-specified options. Features are installed through a feature key that is encoded to work with the serial number of the director. A feature key is a case-sensitive alphanumeric string with dashes every four characters.

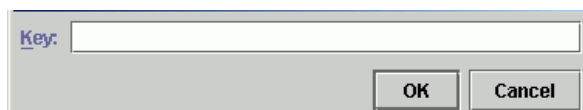
To configure the feature key:

1. Set the director offline ([Set the Director Online or Offline](#) on page 4-43).
2. At the *Hardware View* for the selected director, click *Configure* at top of the view and select *Features* from the pop-up menu. The *Configure Feature Key* dialog box displays ([Figure 2-37](#)).



**Figure 2-37 Configure Feature Key Dialog Box**

3. Click *New*. The *New Feature Key* dialog box displays ([Figure 2-38](#)).



**Figure 2-38 New Feature Key Dialog Box**

4. Type the feature key (case-sensitive xxxx-xxxx-xxxx-xx format) and click *OK*. The *Install Feature Key* dialog box displays ([Figure 2-39](#)).
5. Click *OK*. The director performs an IPL when the feature key is enabled.

**NOTE:** PFE keys are encoded to work only with the serial number of the installed director. Record the key to re-install the feature. If the director must be replaced, obtain new PFE keys from the McDATA Solution Center (800-752-4572 or [support@mcddata.com](mailto:support@mcddata.com)). Have the serial numbers of the old and new directors, and the old PFE key number or transaction code available.

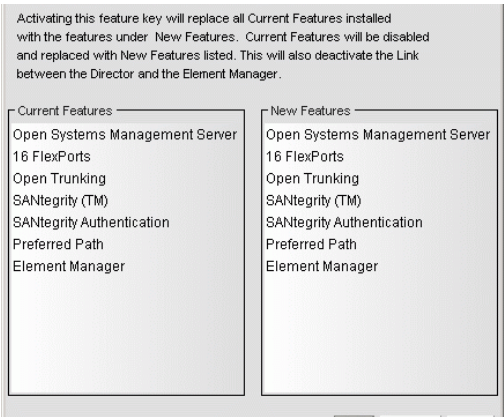


Figure 2-39 Install Feature Key Dialog Box

**Subtask E: Configure Open Systems Management Server (OSMS) or FICON Management Server (FMS)**

Perform this task to configure the open systems management server (OSMS) or FICON management server (FMS). Only one management server can be configured at a time.

**Configure OSMS**

Perform this procedure to configure the open systems management server and enable OSI host control of the director. Implementing host control requires installation of a SAN management application on the OSI server. Management applications include Veritas® SANPoint™ Control (version 1.0 or later), or Tivoli® NetView® (version 6.0 or later).

To configure the open systems management server:

1. At the *Hardware View*, click *Configure* at top of the view and select *Open Systems Management Server* from the pop-up menu. Two submenu options display:
  - *Enable OSMS*.
  - *Host Control Prohibited*.
2. Enable or disable the open systems management server by selecting the *Enable OSMS* option. Check the box to enable the server.
3. Allow or prohibit host (OSI server) control by selecting the *Host Control Prohibited* option. Check the box to prohibit a host management program from changing configuration and connectivity parameters on the director. The host program has read-only access to configuration and connectivity parameters.
4. Click *Activate* to enable a change and allow or prohibit open systems host control.

---

## Configure FMS (FICON)

Perform this procedure to configure the FICON management server and enable FICON host control of the director. Implementing host control requires installation of System Automation for Operating System/390 (SA OS/390), version 1.2 or later.

To configure the FICON management server:

1. At the *Hardware View*, click *Configure* at top of the view and select *FICON Management Server* from the pop-up menu.
2. Enable or disable the following options by clicking the associated check box:
  - **Director Clock Alert Mode** - This option enables or disables a warning message that appears if the director is set to periodically synchronize date and time with the management server. Synchronizing date and time with the management server may conflict with the date and time set from the attached host. If a check mark displays, clock alert mode is enabled.
  - **Programmed offline state control** - This option enables or disables host (S/390 or zSeries 900) ability to set the director offline state. If a check mark displays, control is enabled.

- **Host Control Prohibited** - This option allows or prohibits host (S/390 or zSeries 900) control of the director. If a check mark displays, host control is prohibited.
  - **Active = Saved** - When this option is enabled, the active configuration of logical port addresses is used when the IPL configuration file is updated. If a check mark displays, the *Active = Saved* option is enabled.
3. Select the country code page from the *Code Page* list box. The following selections are available ([Table 2-6](#)).
  4. Click *Activate* to enable changes and allow or prohibit FICON host control.

**Table 2-6 Code Page Table**

Code Page Name	Code Page
United States/Canada	00037
Germany/Austria	00273
Brazil	00275
Italy	00280
Japan	00281
Spain/Latin America	00284
United Kingdom	00285
France	00297
International #5	00500

## Task 8: Configure the Director at the Element Manager Application

To configure the director from the Element Manager application, selectively perform the following configuration tasks according to the customer installation requirements:

- Configure director date and time (*Subtask A: Set Director Date and Time* on page 2-50).
- Identify the director to the SAN management (SANavigator or EFCM) application(*Subtask B: Configure Director Identification* on page 2-51).
- Configure director management style (open systems or FICON) (*Subtask C: Configure Director Management Style* on page 2-52).
- Configure director parameters (*Subtask D: Configure Director Parameters* on page 2-53).
- Configure fabric parameters (*Subtask E: Configure Fabric Parameters* on page 2-55).
- Configure preferred paths (*Subtask F: Configure Preferred Paths* on page 2-57).
- Configure switch binding (*Subtask G: Configure Switch Binding* on page 2-59).
- Configure director ports (*Subtask H: Configure Director Ports* on page 2-63).
- Configure SNMP trap message recipients (*Subtask I: Configure SNMP Trap Message Recipients* on page 2-66).
- Configure threshold alerts (*Subtask J: Configure Threshold Alerts* on page 2-67).
- Configure OpenTrunking (*Subtask K: Configure OpenTrunking* on page 2-71).
- Enable SANpilot interface and Telnet access (*Subtask L: Enable SANpilot Interface and Telnet Access* on page 2-73).
- Configure and enable e-mail notification (*Subtask M: Configure, Enable, and Test E-mail Notification* on page 2-73).
- Configure and enable Ethernet events (*Subtask N: Configure and Enable Ethernet Events* on page 2-75).
- Configure and enable call-home notification (*Subtask O: Configure, Enable, and Test Call-Home Notification* on page 2-76).

## Subtask A: Set Director Date and Time

The director date and time can be set manually, or set to be periodically updated by the SAN management application (the director and application synchronize at least once daily).

At the *Hardware View*, select *Date/Time* from the *Configure* menu. The *Configure Date and Time* dialog box displays (Figure 2-40).

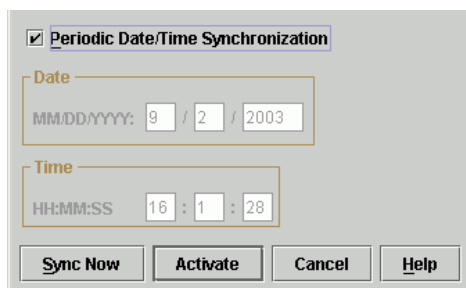


Figure 2-40 Configure Date and Time Dialog Box

### Set Date and Time Manually

To set the director date and time manually:

1. At the *Configure Date and Time* dialog box, click the *Periodic Date/Time Synchronization* check box to deselect the option (no check mark in the box). The greyed out *Date* and *Time* fields activate.
2. Click the *Date* fields that require change, and type numbers in the following ranges:
  - Month (MM): 1 through 12.
  - Day (DD): 1 through 31.
  - Year (YYYY): greater than 1980.
3. Click the *Time* fields that require change, and type numbers in the following ranges:
  - Hour (HH): 0 through 23.
  - Minute (MM): 0 through 59.
  - Second (SS): 0 through 59.
4. Click *Activate* to set the director date and time and close the *Configure Date and Time* dialog box.



## Set Director to Periodically Synchronize Date and Time

To set the director to periodically synchronize date and time with the SAN management application:

- At the *Configure Date and Time* dialog box, click the *Periodic Date/Time Synchronization* check box to select the option (check mark in the box). Perform one of the following:
  - Click *Activate* to enable synchronization and close the *Configure Date and Time* dialog box. The director date and time synchronize with the SAN management application date and time at the next update period (at least once daily).
  - Click *Sync Now* to synchronize the director and SAN management application immediately. The *Date and Time Synced* dialog box displays (Figure 2-41).

Click *OK* to synchronize the date and time and close the *Date and Time Synced* dialog box, then click *Activate* to enable synchronization and close the *Configure Date and Time* dialog box.

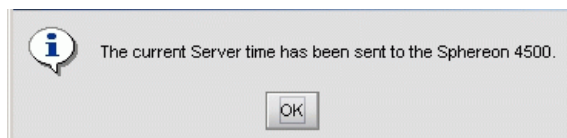


Figure 2-41 Date and Time Synced Dialog Box

## Subtask B: Configure Director Identification

Perform this procedure to configure the director name, description, location, and contact person for the SAN management application.

To configure the director identification:

1. At the *Hardware View*, select *Identification* from the *Configure* menu. The *Configure Identification* dialog box displays (Figure 2-42).

**Figure 2-42 Configure Identification Dialog Box**

- a. Type a director name in the *Name* field. Each director should be configured with a unique name.

If the director is installed on a public LAN, the name should reflect the director Ethernet network DNS host name. For example, if the DNS host name is **intrepid6140.mcdata.com**, the name entered in this dialog box should be **intrepid6140**.

- b. Type a director description in the *Description* field.
- c. Type the director physical location in the *Location* field.
- d. Type the name of a contact person in the *Contact* field.
- e. Click *Set Name as Nickname* to add a check mark to the check box to use the name in the *Name* field as a nickname for the director WWN. The nickname displays instead of the WWN in Element Manager application *Views*.

2. Click *Activate* to save the information and close the window.

## Subtask C: Configure Director Management Style

Perform this procedure to set the director to open systems or FICON management style. This setting only affects the management style used to manage the director and does not affect port operation.

**NOTE:** OSI devices can communicate with each other if the director is set to FICON management style, and FICON devices can communicate with each other if the director is set to open systems management style.

**NOTE:** If the FICON management server feature is enabled, the default management style is FICON. Open systems management style cannot be enabled.

To configure the director management style:

1. Ensure the director is set offline (*Set the Director Online or Offline* on page 4-43).
2. At the *Hardware View* for the selected director, select *Management Style* from the *Product* menu. The *Configure Management Style* menu displays.
3. Select the management style.
  - Select the *Open Systems* radio button for (non-FICON) Fibre channel environments.
  - Select the *FICON* radio button when attaching an IBM S/390 Parallel Enterprise or zSeries server to the director and implementing inband director management through a FICON channel.

---

**NOTE:** If director firmware level is below 6.0 and the FICON Management Server feature is enabled, the default management style will be FICON.

---

---

**NOTE:** The management style cannot be changed to open systems with the FICON Management Server feature enabled.

---

4. Click *Activate* to save the selection and close the window.

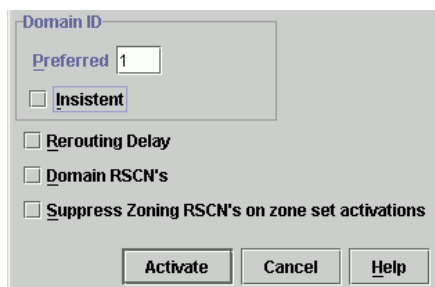
---

## Subtask D: Configure Director Parameters

Perform this procedure to configure director preferred domain ID, insistent domain ID, rerouting delay, and domain RSCNs.

To configure director parameters:

1. Ensure the director is set offline (*Set the Director Online or Offline* on page 4-43).
2. At the *Hardware View* for the selected director, click *Configure* at top of the view. Select *Operating Parameters*, then select *Switch Parameters*. The *Configure Switch Parameters* dialog box displays (*Figure 2-43*).



**Figure 2-43 Configure Switch Parameters Dialog Box**

- a. At the *Preferred Domain ID* field, type a value between 1 through 31. The domain ID uniquely identifies each director or switch in a fabric.

---

**NOTE:** All fabric-attached directors and switches must have unique domain IDs. If the value is not unique, the E\_Port connection to the director segments and the director cannot communicate with the fabric.

---

- b. Click the *Insistent Domain ID* check box to enable this parameter.

When the parameter is enabled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.

- c. Click the *Rerouting Delay* check box to enable this parameter.

When the parameter is enabled, traffic is delayed through the fabric by the specified E\_D\_TOV. This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

- d. Click the *Domain RSCNs* check box to enable this parameter.

When the parameter is enabled, attached devices can register to receive notification when another attached device changes state.

- e. Click the *Suppress RSCNs on zone set activations* check box to enable this parameter.

When the parameter is enabled, attached devices do not receive notification following any change to the fabric active zone set.

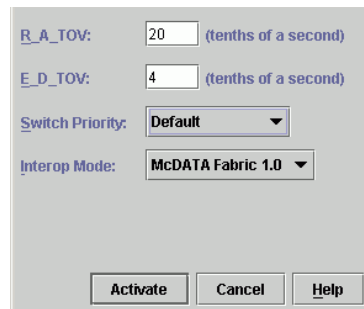
3. Click *Activate* to save the information and close the dialog box.
4. Set the director online ([Set the Director Online or Offline](#) on page 4-43).

## Subtask E: Configure Fabric Parameters

Perform this procedure to configure fabric parameters, including *BB\_Credit*, *R\_A\_TOV*, *E\_D\_TOV*, and switch priority.

To configure fabric parameters:

1. Ensure the director is set offline ([Set the Director Online or Offline](#) on page 4-43).
2. At the *Hardware View* for the selected director, select *Operating Parameters*, then *Fabric Parameters* from the *Configure* menu. The *Configure Fabric Parameters* dialog box displays ([Figure 2-44](#)).



The dialog box is titled "Configure Fabric Parameters". It contains the following fields and controls:

- R\_A\_TOV:** A text input field containing the value "20", followed by the text "(tenths of a second)".
- E\_D\_TOV:** A text input field containing the value "4", followed by the text "(tenths of a second)".
- Switch Priority:** A dropdown menu currently showing "Default".
- Interop Mode:** A dropdown menu currently showing "McDATA Fabric 1.0".

At the bottom of the dialog box are three buttons: "Activate", "Cancel", and "Help".

**Figure 2-44 Configure Fabric Parameters Dialog Box**

- a. At the *BB\_Credit* field, type a value between **1** and **60** buffers. The default is 16.
- b. At the *R\_A\_TOV* field, type a value between **10** and **1200** tenths of a second (one through 120 seconds). The default is 100.

---

**NOTE:** All fabric-attached directors and switches must be set to the same `R_A_TOV`. If the value is not compatible, the `E_Port` connection to the director segments and the director cannot communicate with the fabric. In addition, the `R_A_TOV` must be greater than the `E_D_TOV`.

---

- c. At the `E_D_TOV` field, type a value between **2** and **600** tenths of a second (0.2 through 60 seconds). The default is 20.

---

**NOTE:** All fabric-attached directors and switches must be set to the same `E_D_TOV`. If the value is not compatible, the `E_Port` connection to the director segments and the director cannot communicate with the fabric. In addition, the `E_D_TOV` must be less than the `R_A_TOV`.

---

- d. Set the director priority from the *Switch Priority* drop-down list. Select *Principal*, *Never Principal*, or *Default* (the default is *Default*).

The switch priority value designates the fabric principal switch. The principal switch is assigned a priority of 1 and controls the allocation and distribution of domain IDs for all fabric directors and switches (including itself).

*Principal* is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means that the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a multiswitch fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

- e. Set the director operating mode from the *Interop Mode* drop-down list. This setting only affects the mode used to manage the director and does not affect port operation. Select one of the following options:
- **McDATA Fabric 1.0** - Select this option if the director is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.

- **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the director is fabric-attached to other McDATA directors or switches and open-fabric compliant switches produced by other OEMs.

---

**NOTE:** When Open Fabric 1.0 is selected, the default zone is disabled, and you have to activate the default zone or enable the active zone set

---

3. Click *Activate* to save the information and close the dialog box.
4. Set the director online (*Set the Director Online or Offline* on page 4-43).

---

## Subtask F: Configure Preferred Paths

The preferred path feature allows a user to specify and configure one or more ISL data paths between multiple directors or switches in a fabric. Each participating director or switch must be configured as part of a desired path. The following rules apply when configuring a preferred path:

- The switch domain ID must be set to *Insistent* (*Subtask D: Configure Director Parameters* on page 2-53).
- Domain IDs range between **1** through **31**.
- Source and exit port numbers are limited to the range of ports available on the director.
- For each source port, only one path is defined to each destination domain ID.

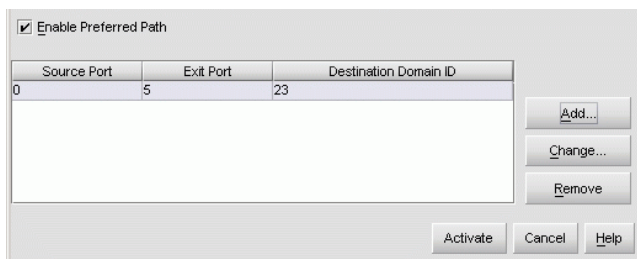
---

**NOTE:** Activating a preferred path can result in receipt of out-of-order frames (OOOFs) if the preferred path differs from the current path, input/output (I/O) is active from the source port, and congestions is present on the current path.

---

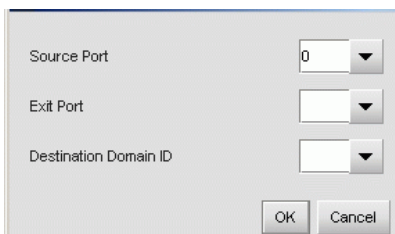
To configure one or more preferred paths for the director:

1. Ensure the preferred path PFE key is installed and configured (*Subtask D: Configure Feature Key* on page 2-45).
2. At the *Hardware View*, select *Preferred Path* from the *Configure* menu. The *Configure Preferred Paths* dialog box displays (*Figure 2-45*).



**Figure 2-45 Configure Preferred Paths Dialog Box**

- Click *Add*. The *Add Preferred Path* dialog box displays (Figure 2-46).



**Figure 2-46 Add Preferred Path Dialog Box**

- At the *Source Port* field, type a value that uniquely identifies the starting port for the preferred path.
- At the *Exit Port* field, type a value that uniquely identifies the exit port for the preferred path.
- At the *Destination Domain ID* field, type a value that uniquely identifies the destination director or switch in the path.
- Click *OK* to close the *Add Preferred Path* dialog box and add the path to the list at the *Configure Preferred Paths* dialog box.
- Repeat [step 3](#) through [step 7](#) to configure additional preferred paths.
- At the *Configure Preferred Paths* dialog box, click the *Enable Preferred Path* check box.
- Click *Activate* to enable all configured preferred paths and close the dialog box.



## Subtask G: Configure Switch Binding

The switch binding (SANtegrity binding) feature specifies devices that can connect to the director ports. This provides security in SAN environments by ensuring that only an intended set of devices can communicate with the director.

### Background: Switch Binding

Specific operating parameters and optional features must be enabled for switch binding to function. In addition, there are requirements for disabling these parameters and features when the director is online or offline, such as:

- Switch binding can be enabled or disabled when the director is either offline or online.
- If Enterprise Fabric Mode is enabled from the SAN management application:
  - Switch binding is automatically enabled.
  - Switch binding cannot be disabled if the director is online.
  - Switch binding can be disabled if the director is offline. However, if switch binding is disabled, Enterprise Fabric Mode is also disabled.
- WWNs can be added to the membership list when switch binding is either enabled or disabled.
- WWNs can be removed from the membership list only if one or more of the following are true:
  - The director is offline.
  - Switch binding is disabled.
  - The associated device is not connected to the director.
  - The associated device is connected to a blocked port.
  - Switch binding is not enabled for the same port type as enabled at the *Switch Binding - Change State* dialog box (Connection Policy). For example, a WWN for a fabric director or switch connected to an E\_Port can be removed if switch binding is enabled to restrict only F\_Ports.

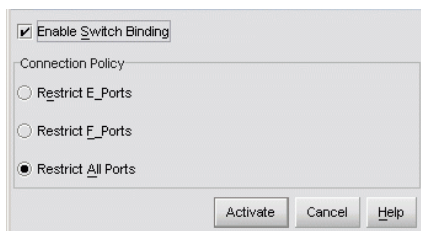
- If the director is online and switch binding is not enabled, all WWNs of devices attached to the director are automatically added to the membership list.

SANtegrity binding parameters have no effect on zoning configurations. However, if a device WWN is in a specific zone, but the WWN is not in the membership list, the device cannot log in to a director port and cannot connect to other devices in the zone with switch binding enabled.

## Enable or Disable Switch Binding

Perform this procedure to configure (enable or disable) switch binding:

1. Ensure the SANtegrity binding feature key is installed and configured (*Subtask D: Configure Feature Key* on page 2-45).
2. At the *Hardware View*, select *Switch Binding*, then *Change State* from the *Configure* menu. The *Switch Binding - Change State* dialog box displays (*Figure 2-47*).



**Figure 2-47 Switch Binding - Change State Dialog Box**

3. Perform one of the following:
  - To enable switch binding, click the *Enable Switch Binding* check box to add a check mark. Go to [step 4](#) to set the connection policy.
  - To disable switch binding, click the *Enable Switch Binding* check box to remove the check mark, then click *Activate* to enable the change and close the dialog box.
4. Select a *Connection Policy* radio button.
  - **Restrict E\_Ports** - Select this button to restrict connections from specific fabric elements to director E\_Ports. WWNs can be added to the membership list to allow element connection

and removed from the list to prohibit element connection. Devices are allowed to connect to any F\_Port or FL\_Port without restriction.

- **Restrict F\_Ports** - Select this button to restrict connections from specific devices to director F\_Ports or FL\_Ports. WWNs can be added to the membership list to allow device connection and removed from the list to prohibit device connection. Fabric directors and switches are allowed to connect to any E\_Port without restriction.
  - **Restrict All** - Select this button to restrict connections from specific devices to director F\_Ports or FL\_Ports and fabric elements to director E\_Ports. WWNs can be added to the membership list to allow connection and removed from the list to prohibit connection.
5. Click *Activate* to enable the changes and close the *Switch Binding - Change State* dialog box.

### Background: Membership List

If the director is online, binding populates a membership list at the *Switch Binding - Membership List* dialog box displays (Figure 2-48) with WWNs of devices connected to the director. The list is modified by the connection policy set in the *Switch Binding - Change State* dialog box (Figure 2-47).

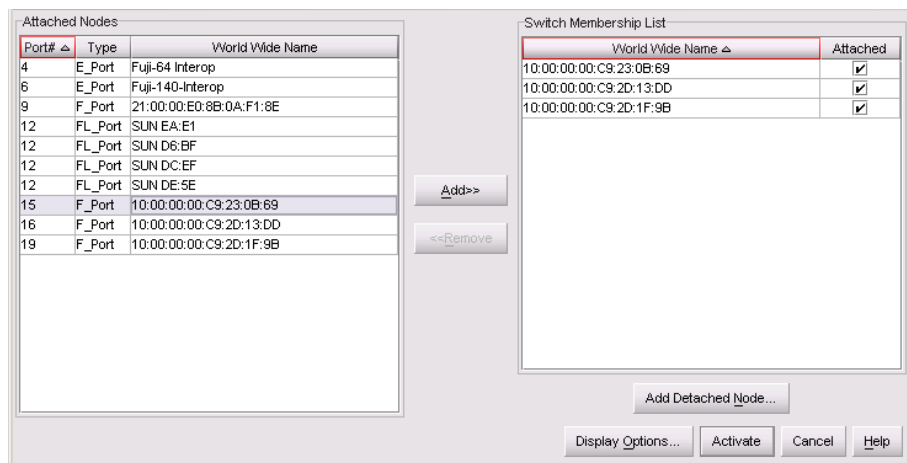


Figure 2-48 Switch Binding - Membership List Dialog Box

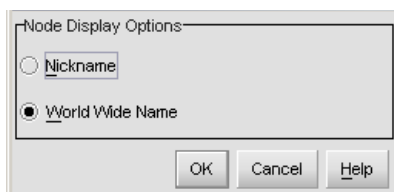
When the switch binding feature is installed but not enabled, the associated membership list is empty. The list is populated with device WWNs:

- When switch binding is enabled with the director online, the membership list is automatically populated with the WWNs of all devices and fabric elements connected to the director.
- When switch binding is enabled with the director offline, the membership list is not automatically populated.
- After enabling switch binding, you can prohibit devices from connecting with director ports by removing the devices from the membership list. Allow devices to connect to director ports by adding the devices to the membership list.

## Edit Membership List

Perform this procedure to edit the switch binding membership list:

1. Ensure the SANtegrity binding feature key is installed and configured ([Subtask D: Configure Feature Key](#) on page 2-45).
2. At the *Hardware View*, select *Switch Binding*, then *Edit Membership List* from the *Configure* menu. The *Switch Binding - Membership List* dialog box displays ([Figure 2-48](#)). WWNs of devices that are allowed to connect to director ports appear in the *Switch Membership List* panel.
3. If nicknames are configured (through the SAN management application) and are to be displayed instead of WWNs, click *Display Options*. The *Display Options* dialog box displays ([Figure 2-49](#)). If nicknames are not configured, go to [step 5](#).



**Figure 2-49** Display Options Dialog Box

4. Click the *Nickname* radio button, then click *OK*. The dialog box closes and nicknames appear in the *Switch Binding - Membership List* dialog box.

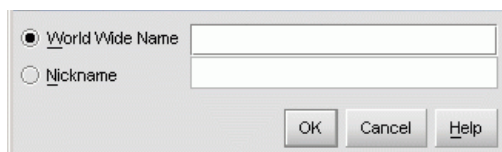
5. Perform one of the following:
  - To allow a director port connection to a device listed in the *Node List Panel*, select the WWN or nickname and click *Add>>*. The device WWN or nickname moves to the *Switch Membership List* panel.
  - To prohibit a director port connection to a device listed in the *Switch Membership List Panel*, select the WWN or nickname and click *<<Remove*. The device WWN or nickname moves to the *Node List* panel.

---

**NOTE:** Device connectivity and membership list edits are subject to the rules defined under [Background: Switch Binding](#) on page 2-59.

---

6. To add a WWN or nickname for a device not connected to the director, click *Detached Node*. The *Add Detached Node* dialog box displays ([Figure 2-50](#)).


 A screenshot of the 'Add Detached Node' dialog box. It features two radio buttons: 'World Wide Name' (selected) and 'Nickname'. Each radio button is followed by a text input field. At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Help'.

**Figure 2-50 Add Detached Node Dialog Box**

7. Type the device WWN or nickname and click *OK*. The WWN or nickname appears in the *Switch Membership List*.
8. Click *Activate* to enable the changes and close the *Switch Binding - Membership List* dialog box.

---

## Subtask H: Configure Director Ports

To configure director Fibre Channel ports:

1. At the *Hardware View*, select *Ports* from the *Configure* menu. The *Configure Ports* dialog box displays ([Figure 2-51](#)).

Port #	Name	Blocked	LIN Alerts	Fan	Type	Speed	Port Binding	Bound WWN
0		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:00:08:00:20:00:00:00
1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:01:00:60:48:00:00:00
2		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:02:00:00:C9:00:00:00
3		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:03:00:60:48:00:00:00
4		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:04:00:00:C9:00:00:00
5		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:05:00:E0:69:00:00:00
6		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:06:00:E0:69:00:00:00
7		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:07:00:60:48:00:00:00
8		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:08:00:E0:69:00:00:00
9		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:09:08:00:20:00:00:00
10		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:0A:08:00:20:00:00:00
11		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:0B:08:00:20:00:00:00
12		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:0C:00:00:C9:00:00:00
13		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:0D:00:00:C9:00:00:00
14		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:0E:00:60:48:00:00:00
15		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:0F:00:00:C9:00:00:00
16		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:10:00:60:48:00:00:00
17		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:11:00:00:C9:00:00:00
18		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:12:00:60:48:00:00:00
19		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:13:00:00:C9:00:00:00
20		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:14:08:00:20:00:00:00
21		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input checked="" type="checkbox"/>	20:15:08:00:20:00:00:00
22		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:16:00:E0:69:00:00:00
23		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	G_Port	1 Gig	<input type="checkbox"/>	20:17:00:00:C9:00:00:00

Figure 2-51 Configure Ports Dialog Box

- For each port to be configured, type a port name in the associated *Name* field. The port name should characterize the device to which the port is attached.
- Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached devices or fabric switch from communicating.
- Click the check box in the *10-100 km* column to enable extended distance buffering for a port (default is disabled). A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.

**NOTE:** If a Director supports BB credits by port, the *10-100 Km* column is replaced by an *RX BB Credit* column.

- If a Director supports BB credits by port, this column displays instead of the *10-100 Km* column. Minimum and maximum allowable port BB credit values vary by Director. If an invalid value is entered, An *Invalid RX BB Credit* error message displays. The BB Credit value is validated as entered. Click *Activate* and a *RX-BB Credit Confirmation* box displays.

In addition to the maximum BB credit limit per port, the total BB credits allocated to all ports cannot exceed the buffer pool size.

**NOTE:** Only 24-Port switches have a switch-wide buffer pool. The *Configure Ports* dialog box displays the total and available buffers at the bottom of the dialog box. When information is changed in the *RX BB Credit* column, this information also updates. If information is entered that exceeds the buffer pool and *Activate* is clicked, an error message displays. Also, ports for the 24-Port switches can be individually configured between 2-12, with a total number of port credits of 150.

Right-clicking in the *RX-BB Credit* column displays a *RX BB Credits* dialog box. For switches without buffer pools, this dialog box allows you to *Set all...* which sets all ports to a single value or *Set all to maximum* which set all ports to a maximum BB credit value. For switches with buffer pools, this dialog box allows you to *Set all...* which sets all ports to a single value or to *Distribute* which evenly distributes the pool buffers among all ports. Clicking *OK* changes the values in the *Configure Port* dialog box. Clicking *Activate* changes the values on the Director.

- e. Clicking *Set all...* displays the *Set All RX BB Credits* dialog box. Entering a value for *RX BB Credit* and clicking *OK* propagates the value to all ports on the *Configure Ports* dialog box. If an invalid value is entered, a message dialog box displays.
  - f. Click the check box in the *LIN Alerts* column to enable or disable link incident (LIN) alerts (default is enabled). A check mark in the box indicates alerts are enabled. When the feature is enabled and an incident occurs on the port link, an alert indicator (yellow triangle) displays at the *Hardware View*, and a message is sent to configured e-mail recipients.
  - g. Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
    - Generic port (**G\_Port**).
    - Fabric port (**F\_Port**).
    - Expansion port (**E\_Port**).
2. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are:
    - Auto-negotiate between 1.0625, 2.125, and 10.625 Gbps operation (**Negotiate**). This is the default.
    - 1.0625 Gbps operation (**1 Gb/sec**).
    - 2.125 Gbps operation (**2 Gb/sec**).

- 10.625 Gbps operation(10 Gb/sec).
- h. Click the check box in the *Port Binding* column to enable or disable port binding (default is disabled). A check mark in the box indicates port binding is enabled and the port can connect only to a device with a WWN listed in the *Bound WWN* column.
- i. If port binding is enabled, type the WWN or nickname of the device attached to the port in the *Bound WWN* column.
  - If the check box in the *Port Binding* column is checked and a WWN or nickname appears in the *Bound WWN* field, only the specified device can attach to the port.
  - If the check box in the *Port Binding* column is checked but no WWN or nickname appears in the *Bound WWN* field, no device can connect to the port.
  - If the check box in the *Port Binding* column is not checked, any device can connect to the port.
- 3. Click *Activate* to save the information and close the *Configure Ports* dialog box.

---

### Subtask I: Configure SNMP Trap Message Recipients

Perform this procedure to configure community names, write authorizations, network addresses, and SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a director event occurs.

To configure SNMP trap recipients:

1. At the *Hardware View* for the selected director, select *SNMP Agent* from the *Configure* menu. The *Configure SNMP* dialog box displays (Figure 2-52).



Community Name	Write Authorization	Trap Recipient	UDP Port Number
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

Activate Cancel Help

**Figure 2-52 Configure SNMP Dialog Box**

- a. For each trap recipient to be configured, type a community name in the associated *Community Name* field. The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
  - b. Click the check box in the *Write Authorization* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark in the box indicates write authorization is enabled. When the feature is enabled, a management workstation user can change the management server *sysContact*, *sysName*, and *sysLocation* SNMP variables.
  - c. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the associated *Trap Recipient* field. It is recommended the IP address be used.
  - d. The default user datagram protocol (UDP) port number for trap recipients is **162**. To override this port number, type a decimal port number in the associated *UDP Port Number* field.
2. To enable transmission of trap messages to configured SNMP workstations, click the *Enable Authorization Traps* check box. A check mark appears in the box when transmission is enabled.
  3. Click *Activate* to save the information and close the dialog box.

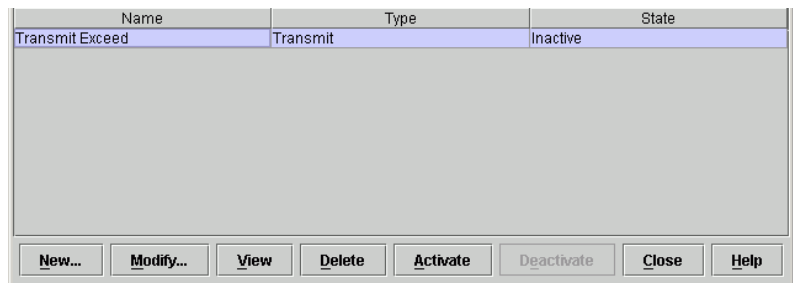
## Subtask J: Configure Threshold Alerts

A threshold alert notifies users when an E\_Port or F\_Port transmit (Tx) or receive (Rx) throughput reaches or exceeds a specified value. Alerts are indicated by:

- An attention indicator (yellow triangle) associated with a port at the *Hardware View*.
- An attention indicator (yellow triangle) in the *Alert* column at the *Port List View*.
- An attention indicator (yellow triangle) in the *Threshold Alerts* field at the *Port Properties* dialog box.
- Data recorded in the *Threshold Alert Log*.

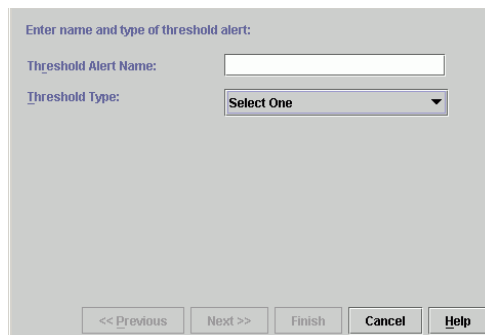
To configure threshold alerts:

1. At the *Hardware View* for the selected director, select *Threshold Alerts* from the *Configure* menu. The *Configure Threshold Alert(s)* dialog box displays ([Figure 2-53](#)).



**Figure 2-53 Configure Threshold Alert(s) Dialog Box**

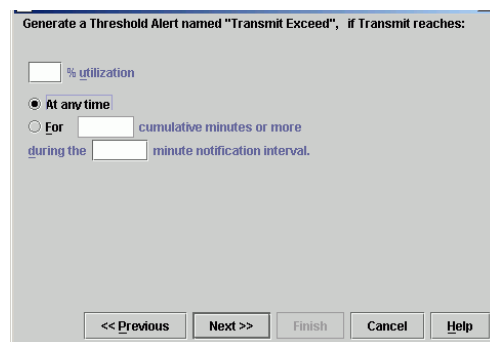
2. Click *New*. The *New Threshold Alert* dialog box (screen 1) displays ([Figure 2-54](#)).



**Figure 2-54 New Threshold Alerts Dialog Box (Screen 1)**

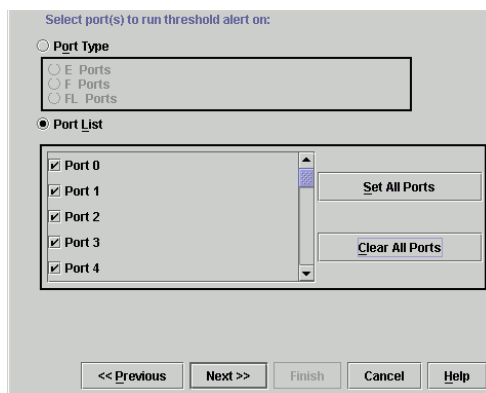
3. Type a name in the *Threshold Alert Name* field.

4. Select one of the following from the drop-down list under the *Threshold Type* field:
  - **Rx Throughput** - An alert occurs if the threshold value for receive throughput is reached or exceeded.
  - **Tx Throughput** - An alert occurs if the threshold value for transmit throughput is reached or exceeded.
  - **Rx or Tx Throughput** - An alert occurs if the threshold value for either receive or transmit throughput is reached or exceeded.
5. Click *Next*. The *New Threshold Alert* dialog box (screen 2) displays (Figure 2-55). The name configured for the alert appears at the top of the dialog box.



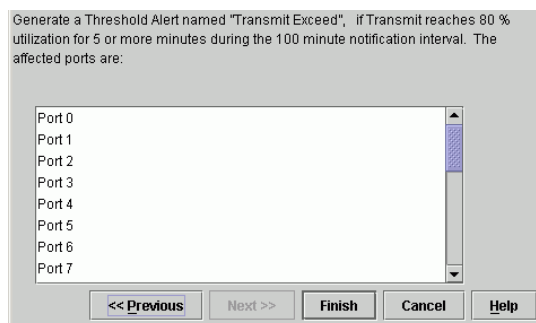
**Figure 2-55 New Threshold Alerts Dialog Box (Screen 2)**

6. Type a percentage from **1** through **100** in the *% utilization* field. When throughput reaches this percentage of port capacity, a threshold alert occurs.
7. Type the cumulative minutes for which the *% utilization* should exist during the notification interval before an alert is generated. Select *At any time* to specify that an alert will occur when the *% utilization* is reached. The valid range is **1** to the interval set in the next step.
8. Type the interval (in minutes) during which throughput is measured and threshold notifications can occur. The valid range is **5** to **70560** minutes.
9. Click *Next*. The *New Threshold Alert* dialog box (screen 3) displays (Figure 2-56).



**Figure 2-56 New Threshold Alerts Dialog Box (Screen 3)**

10. Select the *Port Type* or *Port List* radio button.
  - Select *Port Type* radio button, then the *E\_Ports* or *F\_Ports* radio button to cause an alert to generate for all ports configured as either *E\_Ports* or *F\_Ports*.
  - Select *Port List* to configure individual ports by clicking the check box adjacent to each port number. Select *Set All Ports* to place a check mark adjacent to all port numbers. Select *Clear All Ports* to clear the check marks by port numbers.
11. Click *Next*. The *New Threshold Alert* dialog box (screen 4) displays (Figure 2-57). This screen provides a summary of the alert configuration. To make changes, move back and forth through the configuration screens by selecting *Previous* or *Next*.



**Figure 2-57 New Threshold Alerts Dialog Box (Screen 4)**

12. Click *Finish*. The *Configure Threshold Alerts* dialog box (Figure 2-53) appears listing the name, type, and state of the configured alert.
13. To activate the alert, highlight (select) the alert and click *Activate*.

## Subtask K: Configure OpenTrunking

Perform this procedure to configure the OpenTrunking parameters.

1. Ensure the OpenTrunking feature is installed and configured ([Subtask D: Configure Feature Key](#) on page 2-45).
2. Ensure the director is online ([Set the Director Online or Offline](#) on page 4-43).
3. At the *Hardware View* for the selected director, select *OpenTrunking* from the *Configure* menu. The *Configure OpenTrunking* dialog box displays (Figure 2-58).

Port #	Use Algorithmic Threshold	Threshold %
0	<input checked="" type="checkbox"/>	75
1	<input type="checkbox"/>	65
2	<input type="checkbox"/>	65
3	<input type="checkbox"/>	65
4	<input type="checkbox"/>	65
5	<input type="checkbox"/>	65
6	<input type="checkbox"/>	65
7	<input type="checkbox"/>	65
8	<input type="checkbox"/>	65

Event Notification

☒ Unresolved Congestion

☒ Back Pressure

Low BB Credit Threshold

☒ Default Threshold 45 (1 - 99)%

Activate Cancel Help

Figure 2-58 Configure OpenTrunking Dialog Box

4. Perform one of the following:
  - To enable OpenTrunking, click the *Enable OpenTrunking* check box to add a check mark. Go to [step 5](#) to set the congestion threshold for each port.
  - To disable OpenTrunking, click the *Enable OpenTrunking* check box to remove the check mark, then click *Activate* to enable the change and close the dialog box.

5. For each director port:
  - a. Click the check box in the *Use Algorithmic Threshold* column. A check mark appears in the box and a calculated default value appears (**1% to 99%**) in the associated field in the *Threshold %* column. If the default is enabled, a value cannot be entered in the *Threshold %* column.
  - b. Ensure the check box in the *Use Algorithmic Threshold* column is blank. At the associated field in the *Threshold %* column, type a percentage value from **1% to 99%**.

---

**NOTE:** The default congestion threshold is calculated by the director firmware.

---

6. Click the *Unresolved Congestion* check box to add a check mark and enable the parameter. When this parameter is enabled, unresolved congestion events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

An unresolved congestion event occurs for a low-BB\_Credit ISL when the director rerouting algorithm cannot route data flow to an alternate path (because doing so would exceed the alternate path low BB\_Credit threshold).

7. Click the *Backpressure* check box to add a check mark and enable the parameter. When this parameter is enabled, backpressure events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

A backpressure event occurs when the percent time an ISL has low BB\_Credit exceeds the low BB\_Credit threshold.

8. The low BB\_Credit threshold is the percent time an ISL is allowed to not transmit data because BB\_Credit is unavailable. When the threshold is exceeded, data is rerouted to another ISL. In addition, traffic cannot be rerouted to another low- threshold ISL. Use one of the following to set the low BB\_Credit threshold:
  - Click the *Default Threshold* check box. A check mark appears in the box and a calculated default value appears (**1% to 99%**) in the adjacent field. If the default value is enabled, a value cannot be entered in the field.
  - Ensure the *Default Threshold* check box is blank. At the adjacent field, type a percentage value from **1% to 99%**.

---

**NOTE:** The default low BB\_Credit threshold is calculated by the director firmware.

---

9. Click *Activate* to enable the changes and close the dialog box.

---

### Subtask L: Enable SANpilot Interface and Telnet Access

Perform this procedure to enable the SANpilot interface and Telnet access through the director maintenance port. To enable these functions:

1. To enable the SANpilot interface at the *Hardware View* for the selected director, select *Enable Web Server* from the *Configure* menu. A check mark appears in the box when the interface is enabled, and the menu closes.
2. To enable Telnet access at the *Hardware View* for the selected director, click *Configure* at top of the view and select *Enable Telnet*. A check mark appears in the box when access is enabled, and the menu closes.

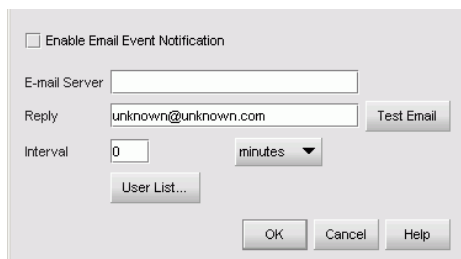
---

### Subtask M: Configure, Enable, and Test E-mail Notification

Perform this procedure to configure, enable, and test e-mail and simple mail transfer protocol (SMTP) addresses to receive notification of director (and other product) events. Configure and test procedures are performed at the SAN management application. E-mail notification is enabled for each director or switch at the Element Manager application.

To configure, enable, and test e-mail addresses:

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.
2. At the EFCM or SANavigator main window, select the *Event Notification* and *Email* options from the *Monitor* menu. The *Email Event Notification Setup* dialog box displays (Figure 2-59).



**Figure 2-59 Email Event Notification Setup Dialog Box**

3. To enable e-mail transmission to configured addresses, click the *Enable Email Event Notification* check box.

---

**NOTE:** The enable function must also be activated for each director or switch through the Intrepid 6140 Element Manager application. E-mail notification can be active for some directors or switches and inactive for others.

---

4. Type the IP address or DNS host name of the SMTP server in the *E-mail Server* field. It is recommended the IP address be used.
5. Type the e-mail address to which e-mail replies should be sent in the *Reply* field.
6. At the *Interval* field, type the length of time the application should wait between notifications. Choose **seconds**, **minutes**, or **hours** from the associated drop-down list.
7. To specify users that are to receive e-mail notification, click *User List*. The *EFCM Server* or *SANavigator Users* dialog box displays (Figure 2-33).
8. To enable e-mail notification for a user, click the check box in the *Email* column.
9. To configure event types for which e-mail notification is sent, click the *Filter* link adjacent to the check box. The *Define Filter* dialog box displays. For instructions on defining event filters, refer to the *McDATA Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153), *McDATA Enterprise Fabric Connectivity Manager User Manual* (620-005001), or *SANavigator User Guide* (621-000013).
10. Click *OK* to close the *EFCM Server* or *SANavigator Users* dialog box.

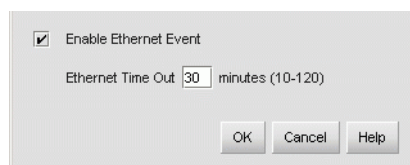


11. Click *Test Email*. A test message is sent to configured e-mail recipients.
12. Click *OK* to save the information and close the *Email Event Notification Setup* dialog box.
13. Maximize the *Hardware View* (Element Manager application).
14. At the *Hardware View*, select *Enable E-Mail Notification* from the *Maintenance* menu. A check mark appears in the check box to indicate e-mail notification for the director is enabled, and the menu closes.

## Subtask N: Configure and Enable Ethernet Events

Perform this procedure to configure and enable Ethernet events. An Ethernet event is recorded (after a user-specified time interval) when the director-to-management server communication link drops. To configure and enable Ethernet events:

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.
2. At the SANavigator or EFCM main window, select the *Ethernet Event* option from the *Monitor* menu. The *Configure Ethernet Events* dialog box displays ([Figure 2-60](#)).



**Figure 2-60** Configure Ethernet Events Dialog Box

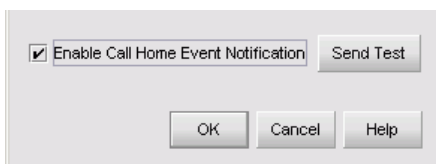
3. Click the *Enable Ethernet Events* check box. A check mark appears in the check box to indicate Ethernet events are enabled.
4. At the *Ethernet Timeout* field, type a value between **10** through **120** minutes.
5. Click *OK* to close the dialog box.

## Subtask O: Configure, Enable, and Test Call-Home Notification

**NOTE:** The call-home feature may not be available if the EFC Manager application (EFCM Lite) is installed on a customer-supplied PC.

Telephone numbers and other information for the call-home feature are configured through the Windows 2000 dial-up networking application. See [Subtask E: Configure the Call-Home Feature](#) on page 2-38 for configuration instructions.

1. Minimize the *Hardware View* (Element Manager application) and return to the SAN management application.
2. At the SANavigator or EFCM main window, select the *Event Notification* and *Call Home* options from the *Monitor* menu. The *Call Home Event Notification Setup* dialog box displays ([Figure 2-61](#)).



**Figure 2-61** Configure Call Home Event Notification Dialog Box

3. Click the *Enable Call Home Event Notification* check box.

**NOTE:** The enable function must also be activated for each director or switch through the director Element Manager application. Call-home event notification can be active for some directors or switches but inactive for others.

4. Click *Send Test*. A call-home test message is sent.
5. Click *OK* to close the dialog box.
6. Maximize the *Hardware View* (Element Manager application).
7. At the *Hardware View*, select *Enable Call Home Notification* from the *Maintenance* menu. A check mark appears in the check box to indicate call-home event notification for the director is enabled, and the menu closes.

---

## Task 9: Configure SANtegrity Authentication (Optional)

This feature is accessed from the *SANtegrity Authentication* Dialog box in the individual element managers applications. The element manager lets you manage one device at a time.

Access the *SANtegrity Authentication* dialog box by clicking the *Configure Menu* on the element manager window and clicking *SANtegrity Authentication*.

To access the *SANtegrity Authentication*, one user must have the security administrator privilege. If not, the *Security* tab is hidden. By default, the security administrator user group displays when installing this feature.

The upper right part of the window shows the main working area, where the security administrator configures the authentication security settings.

The lower left part of the window shows the regular *Master Log* and the lower right part of the window shows the *Security Log*.

---

**NOTE:** The *SANtegrity Authentication* dialog box is only available to the security administrator so the *Security Log* is only available to the security administrator.

---

Change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

On the tool bar the *Display By* option and the *Search Box* option are disabled.

---

### Accessing SANtegrity Authentication

There are five tabs in the *Authentication* section: *Users* tab allows security administrator setup users who accessing the switch from CLI and web interfaces.

- *Software* tab allows the security administrator to setup software applications that can communicate with the switch through API, as well as OSMS authentication.

- *Device* tab allows the security administrator to set device to device authentication parameters. *Device tab* is PFE key enabled. If a proper PFE key is not provided, the *Devices* tab is not accessible.
- *IP Access Control List* tab allows the security administrator to setup IP addresses that can manage the switch.
- *Radius Server* tab allows security administrator to set Radius server parameters that the switch can use to pass on the authentication information to the designated Radius servers.

For complete details on configuring SANtegrity authentication, review the *Element Manager User Manual*.

## Task 10: Back Up Configuration Data

For the EFCM 8.5 application, critical configuration data is stored on the management server hard drive in the following directories:

- **C:\Program Files\EFCM 8.5\CallHome**
- **C:\Program Files\EFCM 8.5\Client**
- **C:\Program Files\EFCM 8.5\Server.**

For the SANavigator 4.1 application, critical configuration data is stored on the management server hard drive in the following directories:

- **C:\Program Files\SANavigator4.1\CallHome**
- **C:\Program Files\SANavigator4.1\Client**
- **C:\Program Files\SANavigator4.1\Server.**

To back up management server configuration data and create a base restore CD:

1. Insert a blank rewritable CD into the CD-RW drive and format the CD.
  - a. At the Windows 2000 desktop, locate the *InCD* icon at the right side of the task bar ([Figure 2-62](#)).



**Figure 2-62 InCD Icon (Unformatted CD)**

- b. Right-click the icon and select *Format (F)*. The the *InCD* wizard window displays.
  - c. Click *Next*. Use the defaults at each window, and click *Next*, then *Finish*, to complete the CD formatting.
  - d. When the CD is formatted, the red down arrow associated with the *InCD* icon changes to a green up arrow.
2. Back up the director configuration file to the management server ([Managing Configuration Data](#) on page 4-74).
3. If the Hardware View is open, close the view and return to the SAN management application (SANavigator or EFCM) by clicking close (X) at the upper right corner of the window.
4. Close the SAN management application by selecting *Shutdown* from the *SAN* menu. An *EFCM* or *SANavigator* dialog box displays.
5. Click *Yes* to close the SAN management application.
6. Reboot the management server to cause directory contents to be written to the blank CD:
  - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.
  - b. Select the *Restart* option from the list box and click *OK*. The management server powers down and restarts. During the reboot, the LAN connection between the management server and PC drops momentarily, and the TightVNC viewer displays a network error.
  - c. After the management server reboots, click *Login again*. The *VNC Authentication* screen displays.
  - d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays.

---

**NOTE:** The default TightVNC viewer password is **password**.

---

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays (Figure 2-16).

---

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action logs the user on to the PC, not the rack-mount management server.

---

- f. Type the default Windows 2000 user name and password and click OK. The management server Windows 2000 desktop opens and the *EFCM* or *SANavigator Log In* dialog box displays (Figure 2-17).

---

**NOTE:** The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- g. Type the SAN management application default user name and password and select a management server or IP address from the *Network Address* drop-down list.

---

**NOTE:** The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- h. Click *Login*. The application opens and the *EFCM* or *SANavigator* main window *View* appears (Figure 2-32).
7. Remove the base restore CD from the CD-RW drive and store the CD in a safe location. Insert a blank rewritable CD into the CD-RW drive and format the CD (step 1).
8. Go to [Task 12: Cable Fibre Channel Ports](#) on page 2-113.

---

## Task 11: Configure the Director at the SANpilot Interface

To configure the director from the SANpilot interface, selectively perform the following configuration tasks according to the customer installation requirements:

- Connect director to Internet or Ethernet LAN segment ([Subtask A: Connect Director to Internet or Ethernet LAN Segment](#) on page 2-82).

- Open the SANpilot interace (*Subtask B: Open the SANpilot Interface* on page 2-82)
- Configure ports (*Subtask C: Configure Director Ports* on page 2-84).
- Configure BB Credits (*Subtask D: Configure BB Credit* on page 2-85).
- Configure director identification (*Subtask E: Configure Director Identification* on page 2-86).
- Configure director date and time (*Subtask F: Configure Date and Time* on page 2-87).
- Configure operating parameters (*Subtask G: Configure Operating Parameters* on page 2-88).
- Configure fabric parameters (*Subtask H: Configure Fabric Parameters* on page 2-91).
- Configure network information (*Subtask I: Configure Network Information* on page 2-93).
- Configure SNMP trap message recipients (*Subtask J: Configure SNMP* on page 2-95).
- Enable command line interface (CLI) and SSH (*Subtask K: Enable or Disable the CLI or SSH* on page 2-97).
- Enable host control (*Subtask L: Enable or Disable OSMS and Host Control* on page 2-98).
- Configure user rights (*Subtask M: Change User Passwords* on page 2-99).
- Configure port binding (*Subtask N: Configure Port Binding* on page 2-100).
- Configure switch binding (*Subtask O: Configure Switch Binding* on page 2-101).
- Configure fabric binding (*Subtask P: Configure Fabric Binding* on page 2-106).
- Enable Enterprise fabric mode (*Subtask Q: Enable or Disable Enterprise Fabric Mode* on page 2-107).
- Configure OpenTrunking (*Subtask R: Configure OpenTrunking* on page 2-108).
- Install feature keys (*Subtask S: Install Feature Keys* on page 2-111).

**NOTE:** In addition to these tasks, there are other tasks which are documented in the SANpilot User Manual and include: Configuring RADIUS Servers, Configuring IP Access Control List, and Configuring Preferred Path. These are advanced topics which are not covered in this document.

### Subtask A: Connect Director to Internet or Ethernet LAN Segment

A PC platform with Internet access and standard web browser running Netscape Navigator® 4.6 or higher or Microsoft Internet Explorer 4.0 or higher is required.

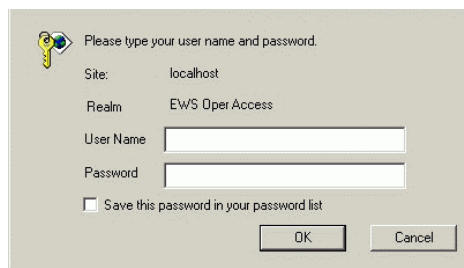
1. Connect one end of the Ethernet patch cable (supplied with the director) to the RJ-45 connector (labelled **10/100**) on the director chassis.
2. Connect the remaining end of the Ethernet cable.
  - Connect the cable to an Internet port or Internet-connected LAN segment as directed by the customer network administrator, or
  - If the McDATA-qualified Ethernet hub provides Internet connectivity, connect the cable to any available hub port.

### Subtask B: Open the SANpilot Interface

To open the SANpilot interface:

1. Ensure the PC and the Ethernet LAN segment (with the director attached) are connected through the Internet.
2. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
3. At the browser, enter the IP address of the director as the Internet uniform resource locator (URL). Use the default IP address of **10.1.1.10**. The *Enter Network Password* dialog box displays (Figure 2-63).



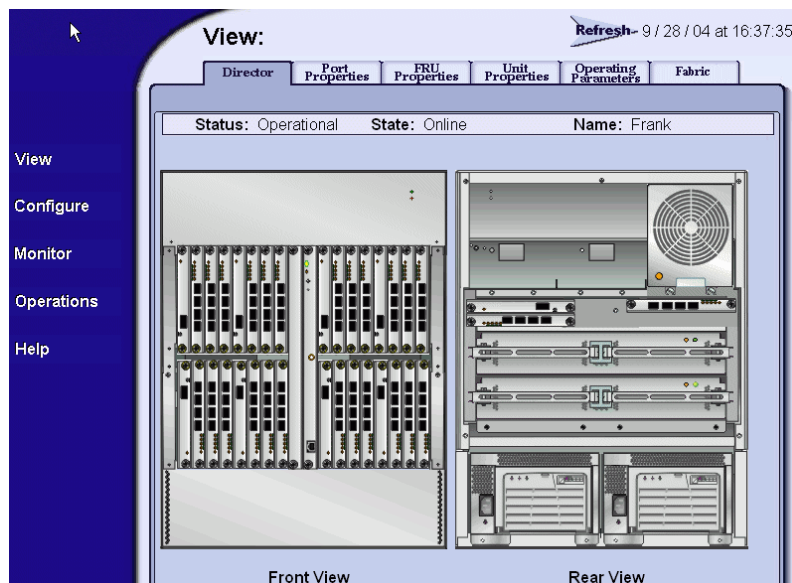


**Figure 2-63 Enter Network Password Dialog Box**

4. Type the default user name and password.

**NOTE:** The default SANpilot interface user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

5. Click OK. The SANpilot interface opens with the *View* panel open and the *Director* page displayed (Figure 2-64).



**Figure 2-64 SANpilot Interface, View Panel (Director Page)**

## Subtask C: Configure Director Ports

Perform procedures in this section to configure names and operating characteristics for Fibre Channel ports.

To configure one or more director ports:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 2-65). Make sure *Basic Info* tab is selected. Use the vertical scroll bar to display additional port information rows.

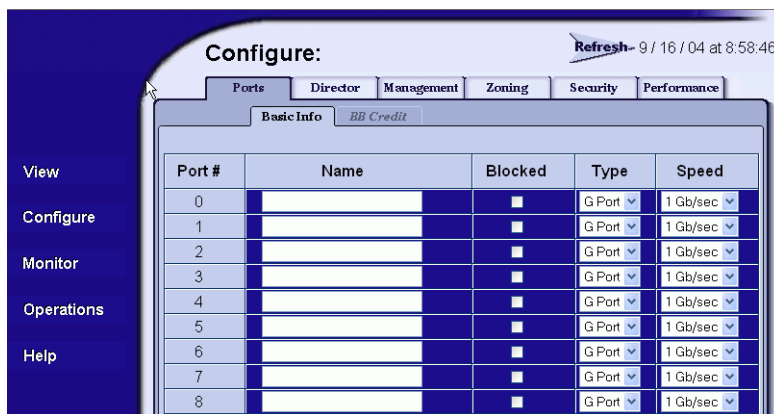


Figure 2-65 Configure Panel (Ports Page)

- a. For each port to be configured, type a port name in the associated *Name* field. The port name should characterize the device to which the port is attached.
- b. Click a check box in the *Blocked* column to block or unblock a port (default is unblocked). A check mark in the box indicates a port is blocked. Blocking a port prevents the attached device or fabric switch from communicating.
- c. Click the check box in the *10-100 km* column to enable extended distance buffering for a port (default is disabled). A check mark in the box indicates extended distance operation up to 100 kilometers (through repeaters) is enabled.
- d. Select from the drop-down list in the *Type* column to configure the port type. Available selections are:
  - Generic port (**G\_Port**).

- Fabric port (**F\_Port**).
  - Expansion port (**E\_Port**).
- e. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are:
- Auto-negotiate between 1.0625, 2.125, and 10.625 Gbps operation (**Negotiate**). This is the default.
  - 1.0625 Gbps operation (**1 Gb/sec**).
  - 2.125 Gbps operation (**2 Gb/sec**).
  - 10.625 Gbps operation (**10 Gb/sec**).
2. Click *Activate* to save and activate the changes. The message **Your changes to the port configuration have been successfully activated** appears.

---

### Subtask D: Configure BB Credit

Perform this procedure to configure the BB Credit allocation for all ports on the product. For each type of port, there is a maximum and minimum BB Credit limit which is displayed as a range. To configure the BB Credit allocation, the port must be set to offline. The simplest way to set the port to offline is to block the port. As you enter the BB Credit value, the value will be validated and an error message will be displayed for each port if applicable. The BB Credit configuration will not be activated if there are any outstanding errors.

To configure BB credits:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed ([Figure 2-65](#)). Select the *BB Credits* tab is selected. Use the vertical scroll bar to display additional port information rows.
2. It is recommended you select the Default values. If not, you can enter values in the RX BB Credit field.
3. Select *Activate* to save the changes.
4. Place the port back online.

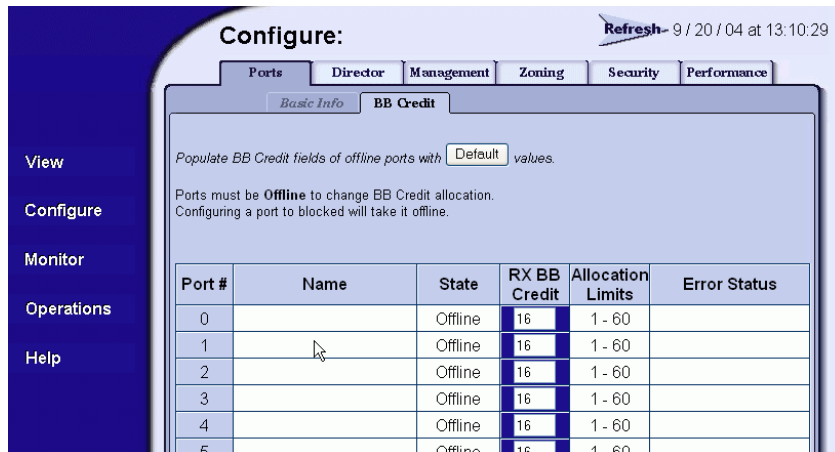


Figure 2-66 Configure BB Credits

## Subtask E: Configure Director Identification

Perform this procedure to configure the director name, description, location, and contact person. The *Name*, *Location*, and *Contact* variables configured correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*. These variables are used by SNMP management workstations when obtaining data from managed directors.

To configure the director identification:

1. At the *Configure* panel, click the *Director* tab. The *Director* page displays with *Identification* selected (Figure 2-67).

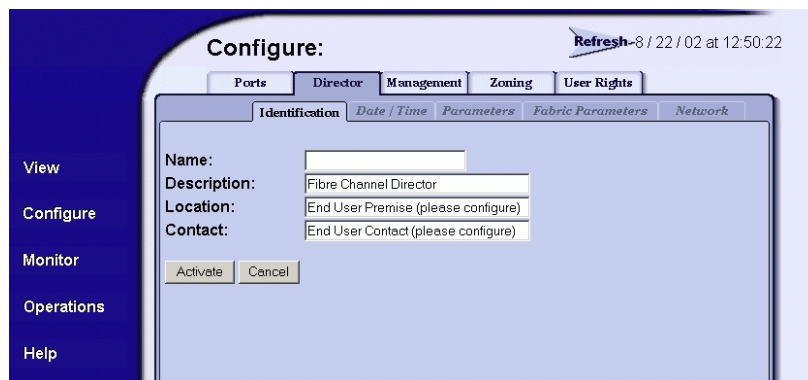


Figure 2-67 Configure Panel (Director Page with Identification Tab)

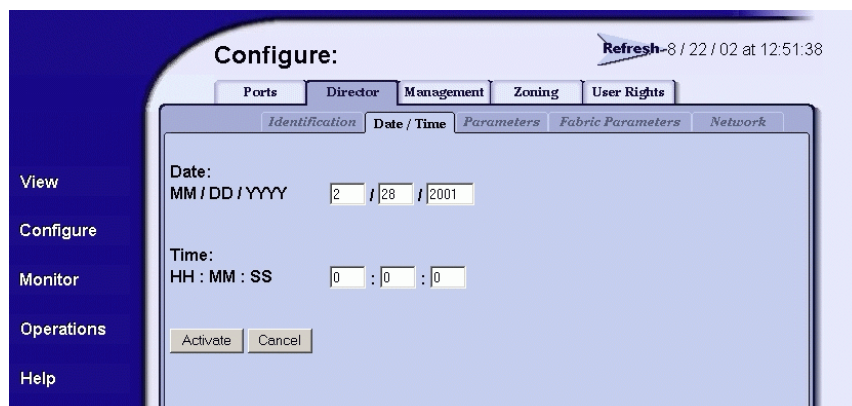
- a. Type a director name in the *Name* field. Each director or switch should be configured with a unique name. The director name can be up to 24 alphanumeric characters and you can use spaces in the name.  
  
If the director is installed on a public LAN, the name should reflect the director Ethernet network domain name system (DNS) host name. For example, if the DNS host name is **intrepid6140.mcddata.com**, the name entered in this dialog box should be **intrepid6140**.
- b. Type a director description up to 255 alphanumeric characters in the *Description* field.
- c. Type the director physical location up to 255 alphanumeric characters in the *Location* field.
- d. Type the name of a contact person up to 255 alphanumeric characters in the *Contact* field.
2. Click *Activate* to save and activate the changes. The message **Your changes to the identification configuration have been successfully activated** appears.

## Subtask F: Configure Date and Time

Perform this procedure to configure the effective date and time for the director.

To set the date and time:

1. At the *Configure* panel, click the *Date/Time* tab. The *Director* page displays with *Date/Time* selected (Figure 2-68).



**Figure 2-68 Configure Panel (Director Page with Date/Time Tab)**

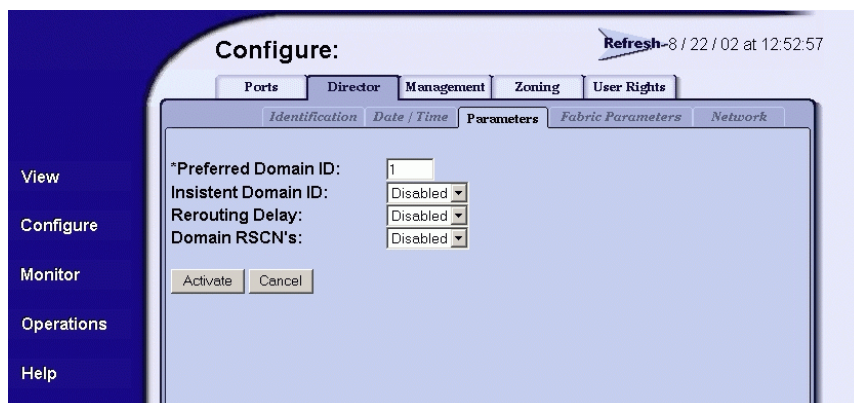
- a. Click the *Date* fields that require change, and type numbers in the following ranges:
    - Month (*MM*): 1 through 12.
    - Day (*DD*): 1 through 31.
    - Year (*YYYY*): greater than 1980.
  - b. Click the *Time* fields that require change, and type numbers in the following ranges:
    - Hour (*HH*): 0 through 23.
    - Minute (*MM*): 0 through 59.
    - Second (*SS*): 0 through 59.
2. Click *Activate* to save and activate the changes. The message **Your changes to the date/time configuration have been successfully activated** appears.

## Subtask G: Configure Operating Parameters

Perform this procedure to configure the director preferred domain ID, insistent domain ID, rerouting delay, and domain registered state change notifications (RSCNs).

To configure parameters:

1. Set the director offline.
  - a. At the *Configure* panel, select *Operations* at the left side of the panel. The *Operations* panel opens and the *Director* page displays with the *Beacon* tab selected
  - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Director* tab, then select *Parameters*. The *Director* page displays with *Parameters* selected (Figure 2-69).



**Figure 2-69 Configure Panel (Director Page with Parameters Tab)**

- a. At the *Preferred Domain ID* field, type a value between 1 through 31. The domain ID uniquely identifies each director or switch in a fabric.

---

**NOTE:** If the director is attached to a fabric element, the director and element must have unique domain IDs. If the values are not unique, the E\_Port connection to the element segments and the director cannot communicate with the fabric.

---

- b. At the *Insistent Domain ID* field, select *Enabled* or *Disabled*. When this parameter is enabled, the domain ID configured in the *Preferred Domain ID* field becomes the active domain identification when the fabric initializes.

---

**NOTE:** If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Insistent Domain ID must be enabled.

---

- c. At the *Rerouting Delay* field, select *Enabled* or *Disabled*. When this parameter is enabled, traffic is delayed through the fabric by the specified error detect time out value (E\_D\_TOV). This delay ensures Fibre Channel frames are delivered to their destination in order, even if a change to the fabric topology creates a new (shorter) transmission path.

---

**NOTE:** If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Rerouting Delay must be enabled.

---

- d. At the *Domain RSCNs* field, select *Enabled* or *Disabled*. When this parameter is enabled, attached devices can register to receive notification when another attached device changes state.

---

**NOTE:** If Enterprise Fabric Mode (an optional SANtegrity Binding feature) or Fabric Binding is enabled, then Domain RSCN must be enabled.

---

- e. At the *Suppress RSCN on Zone Set Activations* field, select *Enabled* or *Disabled*. When this parameter is enabled, RSCN messages are prohibited from being sent to ports on the switch following any change to the fabric's active zone set.
4. Click *Activate* to save and activate the changes. The message **Your changes to the operating parameters configuration have been successfully activated** appears.
  5. If fabric parameters require configuration, go to [Subtask H: Configure Fabric Parameters](#) following. If the configuration is complete, set the director online.
    - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Director* page displays with the *Beacon* tab selected



- b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

## Subtask H: Configure Fabric Parameters

Perform this procedure to configure the fabric operating parameters, including resource allocation time out value ( R\_A\_TOV), E\_D\_TOV, switch priority, and interop mode.

To configure parameters:

1. If required, set the director offline.
  - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Director* page displays with the *Beacon* tab selected
  - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
3. At the *Configure* panel, click the *Director* tab, then click the *Fabric Parameters* tab. The *Director* page displays with the *Fabric Parameters* tab selected (Figure 2-70).

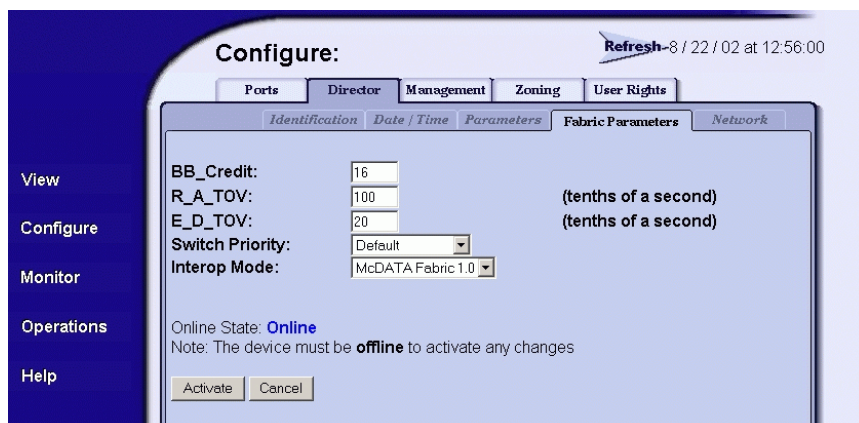


Figure 2-70 Configure Panel (Director Page with Fabric Parameters Tab)

- a. At the *R\_A\_TOV* field, type a value between **10** through **1200** tenths of a second (1 through 120 seconds). Ten seconds (**100**) is the recommended value.

---

**NOTE:** If the director is attached to a fabric element, the director and element must be set to the same *R\_A\_TOV* value. If the values are not identical, the *E\_Port* connection to the element segments and the director cannot communicate with the fabric. In addition, the *R\_A\_TOV* value must be greater than the *E\_D\_TOV* value.

---

- b. At the *E\_D\_TOV* field, type a value between **2** through **600** tenths of a second (0.2 through 60 seconds). Two seconds (**20**) is the recommended value.

---

**NOTE:** If the director is attached to a fabric element, the director and element must be set to the same *E\_D\_TOV* value. If the values are not identical, the *E\_Port* connection to the element segments and the director cannot communicate with the fabric. In addition, the *E\_D\_TOV* value must be less than the *R\_A\_TOV* value.

---

- c. Select from the *Switch Priority* drop-down list to set the director or switch priority. Available selections are *Default*, *Principal*, and *Never Principal*. The default setting is *Default*.

This value designates the fabric principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

*Principal* is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest world wide name (WWN) becomes the principal switch.

At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all interswitch links (ISLs) segment.

- d. Select from the *Interop Mode* drop-down list to set the switch operating mode. This setting only affects the mode used to manage the director or switch; it does not affect port operation. Available selections are:

- **McDATA Fabric 1.0** - Select this option if the director is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
  - **Open Fabric 1.0** - Select this option (default) for managing heterogeneous fabrics and if the director is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other original equipment manufacturers (OEMs).
4. Click *Activate* to save and activate the changes. The message **Your changes to the fabric parameters configuration have been successfully activated** appears.
  5. Set the director online.
    - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
    - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

---

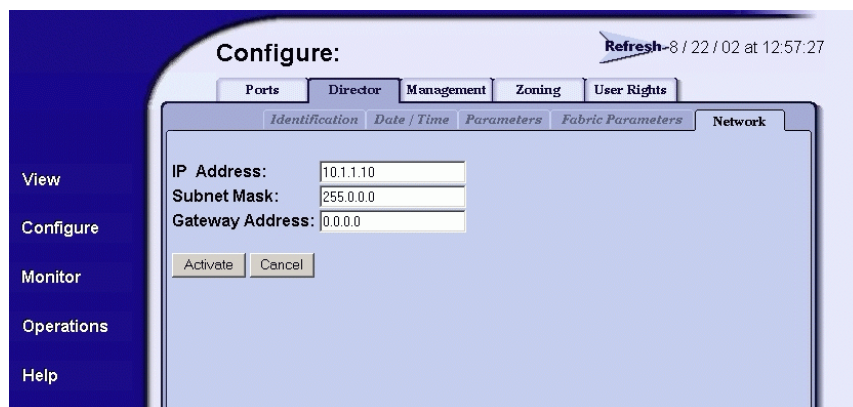
## Subtask I: Configure Network Information

Verify the type of LAN installation with the customer network administrator. If one director is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change. Go to [Subtask J: Configure SNMP](#) on page 2-95.

If multiple directors or switches are installed or a public LAN segment is used, network information must be changed to conform to the customer LAN addressing plan.

To change a director IP address, subnet mask, or gateway address:

1. At the *Operations* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
2. At the *Configure* panel, click the *Director* tab, then click the *Network* tab. The *Director* page displays with the *Network* tab selected ([Figure 2-71](#)).



**Figure 2-71 Configure Panel (Director Page with Network Tab)**

- a. At the *IP Address* field, type the new value as specified by the customer network administrator (default is **10.1.1.10**).
- b. At the *Subnet Mask* field, type the new value as specified by the customer network administrator (default is **255.0.0.0**).
- c. At the *Gateway Address* field, type the new value as specified by the customer network administrator (default is **0.0.0.0**).
3. Click *Activate* to save and activate the changes.
4. Update the address resolution protocol (ARP) table for the browser PC.
  - a. Select the *Exit* option from the *File* menu to close the SANpilot interface and browser applications. The Windows desktop displays.
  - b. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.
  - c. At the *Windows Workstation* menu, sequentially select the *Programs* and *Command Prompt* options. A disk operating system (DOS) window displays.
  - d. Delete the director *old* IP address from the ARP table. At the command (C:\) prompt, type **arp -d xxx.xxx.xxx.xxx**, where *xxx.xxx.xxx.xxx* is the old IP address for the director.
  - e. Click close (X) at the upper right corner of the DOS window to close the window and return to the Windows desktop.

5. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
6. At the browser, enter the director *new* IP address as the Internet URL. The *Enter Network Password* dialog box displays.
7. Type the default user name and password.

---

**NOTE:** The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

8. Click OK. The SANpilot interface opens with the *View* panel open and the *Director* page displayed.
9. IML the director (*IML, IPL, or Reset the Director* on page 4-53).

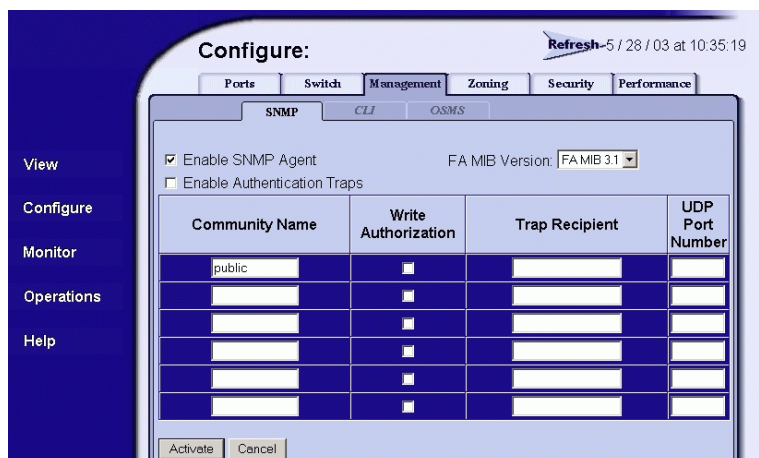
---

## Subtask J: Configure SNMP

Perform this procedure to configure community names, write authorizations, network addresses, and user datagram protocol (UDP) port numbers for SNMP trap message recipients. A trap recipient is a management workstation that receives notification (through SNMP) if a director event occurs.

To configure SNMP trap recipients:

1. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed.
2. At the *Configure* panel, click the *Management* tab. The *Management* page displays with the *SNMP* tab selected ([Figure 2-72](#)).



**Figure 2-72 Configure Panel (Management Page with SNMP Tab)**

- Click the *Enable SNMP Agent* check box to enable or disable the installed SNMP agent.
- Select the Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. This should be set to match the level of FA MIB used by the SNMP management stations that access the product.
- Click the *Enable Authentication Traps* check box to enable or disable transmission of SNMP trap messages to configured recipients.
- For each trap recipient to be configured, type a community name in the *Community Name* field of less than 32 alphanumeric characters (you can use spaces in the community name field). The community name is incorporated in SNMP trap messages to ensure against unauthorized viewing or use.
- Click the check box in the *Write Authorization* column to enable or disable write authorization for the trap recipient (default is disabled). A check mark indicates write authorization is enabled. When the feature is enabled, a management workstation user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

- f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field in four-byte, dotted-decimal format with a maximum of 16 characters. It is recommended the IP address be used.
- g. The default UDP port number for trap recipients is **162**. Type a decimal port number in the *UDP Port Number* field to override the default value. The range for the UDP port number value is 1 to 65535.
3. Click *Activate* to save and activate the changes. The message **Your changes to the SNMP configuration have been successfully activated** appears.

### Subtask K: Enable or Disable the CLI or SSH

Perform this procedure to toggle (enable or disable) the state of the director command line interface (CLI) as well as the configuration of the secure shell which is used to provide secure access and encrypted data when using the Telnet function.

To change the CLI state:

1. At the *Configure* panel, click the *CLI* tab. The *Management* page displays with the *CLI* tab selected (Figure 2-73).

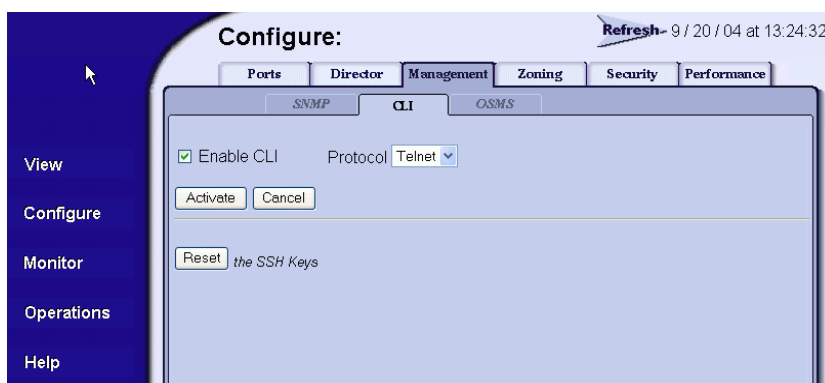


Figure 2-73 Configure Panel (Management Page with CLI Tab)

2. Perform one of the following steps:

- Click *Enable* to activate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.
  - Click *Disable* to deactivate the CLI. The message **Your changes to the CLI enable state have been successfully activated** appears.
3. To enable SSH, from the *Protocol* drop down box, select *SSH*.
  4. Select *Activate* to enable SSH for Telnet.

---

**NOTE:** The default value is Telnet which means that data is not encrypted between the user and the product. By selecting SSH, data, such as a user ID and password, is encrypted between the user and the product.

---

---

### Subtask L: Enable or Disable OSMS and Host Control

Perform this procedure to toggle (enable or disable) host control of the director through the OSMS. The OSMS feature must be installed to access this control ([Subtask S: Install Feature Keys](#) on page 2-111). If the feature is not installed, the message **OSMS Feature Not Installed** appears.

To enable or disable OSMS:

1. At the *Configure* panel, click the *Managment* tab and then the *OSMS* tab. The *Management* page displays with the *OSMS* tab selected ([Figure 2-74](#)).



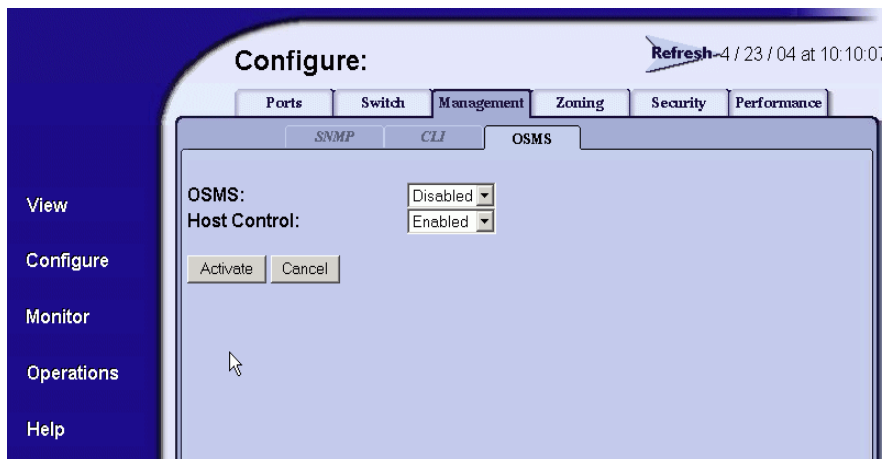


Figure 2-74 Configure Panel (Management Page with OSMS Tab)

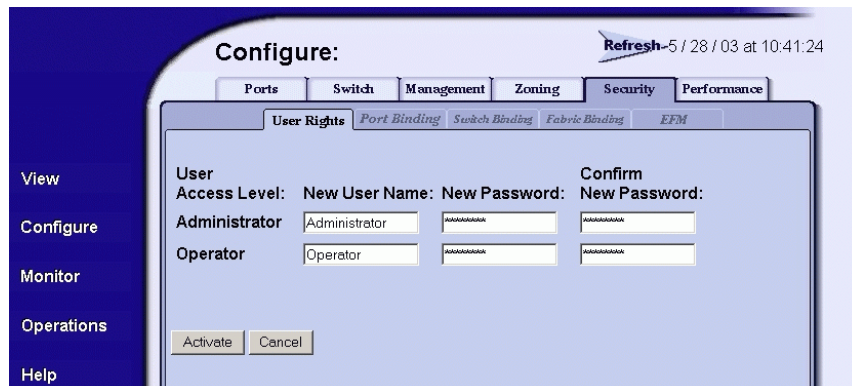
2. Select either Enable or Disable from the drop-down box:
  - Select *Enable* to activate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.
  - Select *Disable* to deactivate the OSMS. The message **Your changes to the host control enable state have been successfully activated** appears.
3. To change the host control state, select enable or disable from the drop-down box. Before you can enable host control state, OSMS must be enabled.

### Subtask M: Change User Passwords

Perform this procedure to change the administrator-level and operator-level passwords used to access the SANpilot interface through the *Enter Network Password* dialog box.

To configure passwords:

1. At the *Configure* panel, click the *Security* tab. The *Security* page displays with the *Authorize Users* tab selected (Figure 2-75).



**Figure 2-75 Configure Panel (Security Page with User Rights Tab)**

2. Under the Currer User Records, enter the new password.
3. Click *Activate* to save the information. The message **Your changes to the user rights configuration have been successfully activated** appears.

**NOTE:** If you want to create a user account, review the SANpilot User's Guide for more information. Before you create a new user, you should review information on the security features provided with SANtegrity and RADIUS Servers such as authentication for the various interfaces such as Web (HTTP), CLI, Serial Port, E Port, N Port, and OSMS.

## Subtask N: Configure Port Binding

Perform this procedure to configure Fibre Channel port binding by WWN.

To configure port binding:

1. At the *Configure* panel, click the *Port Binding* tab. The *Security* page displays with the *Port Binding* tab selected ([Figure 2-76](#)).

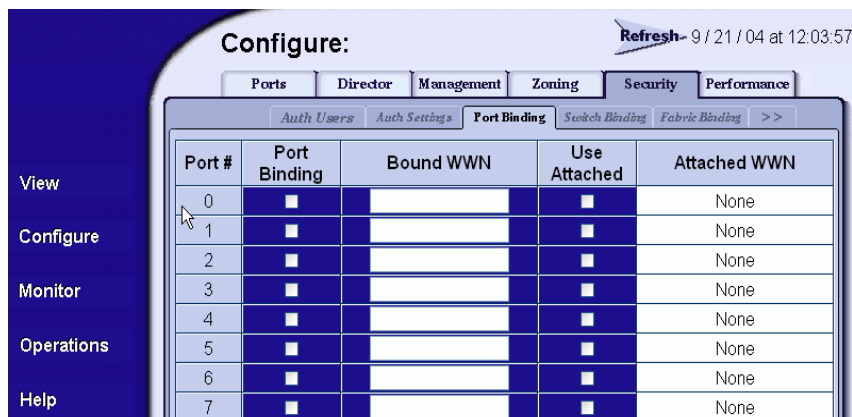


Figure 2-76 Configure Panel (Security Page with Port Binding Tab)

- a. Click the check box in the *Port Binding* column to enable or disable port binding for a specified port (default is disabled).
  - b. In the *Bound WWN* column, type the world wide name of the device to which the port is to be bound. If port binding is enabled, only the specified device can connect to the port. If port binding is enabled and no device is specified in the *Bound WWN* column, then no devices can connect to the port.
  - c. The *Attached WWN* column contains read-only fields that list the world wide names of attached Fibre Channel devices. Click the check box in the *Use Attached* column to indicate the world wide name specified in the *Attached WWN* column is to be used for port binding. After activation, the attached WWN appears in the *Bound WWN* column.
2. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.

## Subtask O: Configure Switch Binding

Perform this procedure to configure switch binding by attached devices (nodes). The SANtegrity feature must be installed to access this control ([Subtask S: Install Feature Keys](#) on page 2-111). If the feature is not installed, the message **This Feature Not Installed** appears.

Switch Binding functionality enables you to identify the devices with which the switch or director can communicate. Switch Binding is available only if the SANtegrity Binding feature is installed.

The *Switch Binding* tab view allows you to enable the product to communicate only with devices that are listed on the Switch Binding Membership List (SBML). Switch Binding restricts connections to only the devices listed on the SBML and allows no other devices to communicate with the switch. When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the event log. This provides security in environments that include a large number of devices by ensuring that only the specified set of devices are able to attach to a switch or director.

You can use the *Switch Binding* tab to enable Switch Binding and to create and change the SBML.

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features:

- Switch Binding can be enabled or disabled whether the product is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is offline you can disable Switch Binding, but this also disables Enterprise Fabric Mode.
- WWNs can be added to the SBML without regard to whether Switch Binding is enabled or disabled.
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the SBML.

To configure switch binding:

1. At the *Configure* panel, click the *Switch Binding* tab. The *Security* page displays with the *Switch Binding* tab selected ([Figure 2-77](#)).

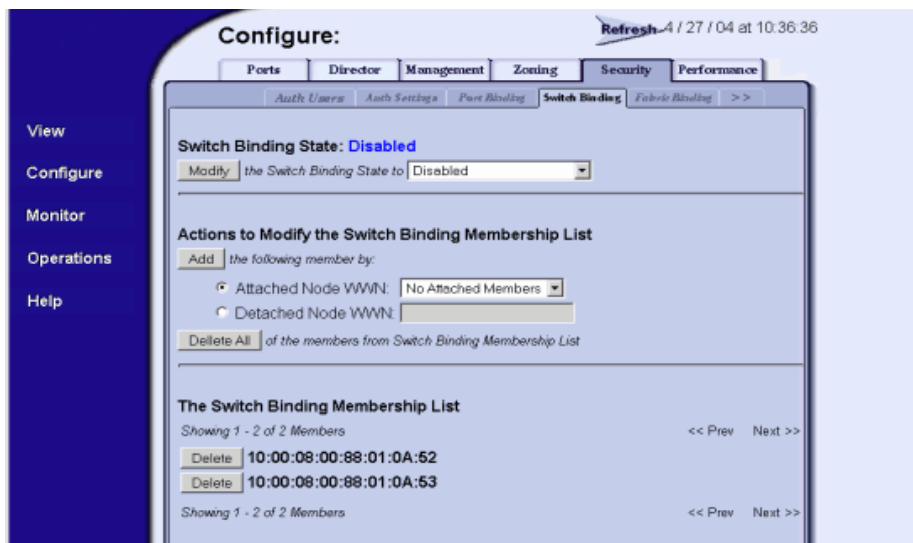


Figure 2-77 Configure Panel (Security Page with Switch Binding Tab)

2. Select the connection policy from the *Switch Binding State* drop-down list. The switch binding state indicates the type of binding restrictions imposed on the director. Switch binding is enabled by activating Enterprise Fabric Mode ([Subtask Q: Enable or Disable Enterprise Fabric Mode](#) on page 2-107) or by enforcing a connection policy at the *Switch Binding State* drop-down list. Available selections are:
  - **Enable & Restrict E\_Ports** - Uses the switch binding membership list to restrict devices that can attach to the director through E\_Ports.
  - **Enable & Restrict F\_Ports** - Uses the switch binding membership list to restrict devices that can attach to the director through F\_Ports.
  - **Enable & Restrict All Ports** - Uses the switch binding membership list to restrict devices that can attach to the director through any port.
  - **Disable Switch Binding** - Sets the switch binding state to disabled and removes restrictions on devices that can attach to the director.

3. Click *Submit*. A confirmation dialog box appears. Click *OK* to close the confirmation dialog box, activate the selected connection policy, and change the switch binding state.

---

**NOTE:** The **Disable Switch Binding** selection cannot be activated while Enterprise Fabric Mode is enabled and the director is online.

---

4. The *Attached Nodes* drop-down list contains the world wide names of attached Fibre Channel devices. To add a member (node or device) to the switch binding membership list displayed at the bottom of the page, perform one of the following:
  - Select a WWN from the *Attached Nodes* drop-down list and click the adjacent *Add Member* button.
  - Type a new WWN in the *Detached Node (WWN)* field and click the adjacent *Add Member* button.
5. To delete a device from the switch binding membership list, click the *Delete* button adjacent to the device WWN. A confirmation dialog box appears. Click *OK* to close the dialog box and delete the device.

---

## Configuring the Switch Binding Membership List

The SBML contains the WWNs of devices that are allowed to communicate with the switch when Switch Binding is enabled. This list is configured using the *Switch Binding* tab.

The contents of the SBML are shown at the bottom of the tab, listed by WWN. The tab can show up to 64 list members. If the list contains more than 64 members, the other list members are shown on subsequent pages. To see the next page of list members, click the *Display More Members* option. To see the previous page of list members, click the *Display Previous Members* option. The message *All Members Displayed* appears on the last page of entries.

## Adding a List Member

To add a new member to the SBML, perform the following procedure:

1. Select *Configure* from the navigation panel.
2. Select the *Security* tab and the *Switch Binding* tab.
3. Add the node to the list in one of the following ways:
  - Select an attached node from the *Attached Node WWN* drop down list.

- If you select *Detached Node* WWN, type the WWN of a detached node. The WWN must be entered as hex digits, all uppercase, and with no colon separator between digits.
4. Select the *Add the following member by* button next to the node that you wish to add. The tab view refreshes and the node is now listed in the SBML at the bottom of the screen.
  5. If a duplicate member is submitted for the membership list, an error message is displayed that an invalid membership list has been submitted.

### Deleting a List Member

WWNs can only be removed from the SBML if any of the following are true:

- The director or switch is offline.
- Switch Binding is disabled.
- The switch or device with the WWN is not currently connected to the director or switch (detached node).
- Switch Binding is not enabled for the same port type as enabled for the connection policy. For example, a WWN for a switch attached to an E\_Port can be removed if the Switch Binding connection policy is set to *Enabled & Restrict F\_Ports*.
- The switch or device with the WWN is connected to a port that is blocked.

To delete a member or all members from the SBML, perform the following procedure:

1. Select *Configure* from the navigation panel.
2. Select the *Security* tab and the *Switch Binding* tab.
3. Select the *Delete* button next to the listing for the member.
4. At the *Are you sure you want to delete this member?* prompt, click *OK*. The SBML redisplay without the deleted member.
5. If you want to delete all of the members of a switch binding membership list, select *Delete All Members from the Switch Binding Membership List*.

## Subtask P: Configure Fabric Binding

Perform this procedure to configure fabric binding by attached fabric member (domain ID and WWN). The SANtegrity feature must be installed to access this control (*Subtask S: Install Feature Keys* on page 2-111). If the feature is not installed, the message **This Feature Not Installed** appears.

To configure fabric binding:

1. At the *Configure* panel, click the *Fabric Binding* tab. The *Security* page displays with the *Fabric Binding* tab selected (Figure 2-78).

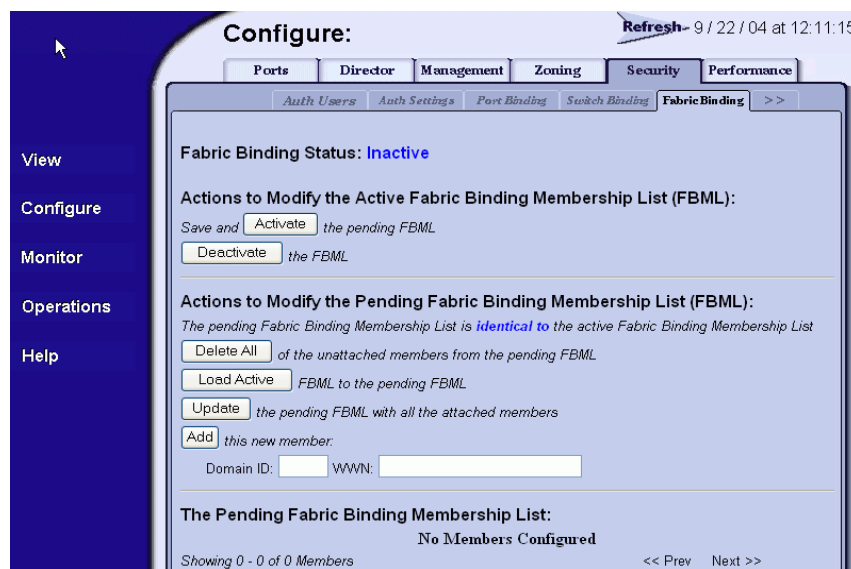


Figure 2-78 Configure Panel (Security Page with Fabric Binding Tab)

2. The Fabric Binding tab is divided into sections by the following headings. Configure fabric binding from the following:
  - Fabric Binding Status—Identifies whether Fabric Binding is active or inactive on the product.
  - Actions to Modify the Active Fabric Binding Membership List (FBML)—Enables you to activate and deactivate Fabric Binding using the following buttons:
    - Activate: By selecting this button, you save the pending FBML as the active FBML and activate Fabric Binding.



- Deactivate: By selecting this button, you change the Fabric Binding status from active to inactive, disabling Fabric Binding.
- Actions to Modify the Pending Fabric Binding Membership List (FBML)—Enables you to modify the pending FBML using the following buttons:
  - Delete All: By selecting this button, you can delete all members from the pending FBML that are not attached to the current fabric. Members that are attached must remain in the list, because the membership list must contain all attached members to be activated.
  - Load Active: By selecting this button, you can copy the contents of the active FBML to the pending FBML. The added members may include unattached members of the active FBML.
  - Update: By selecting this button, you can update the pending FBML to include all currently attached fabric members. Unattached members of the active FBML are not added to the list by this action.
  - Add: By selecting this button, you can add a new member to the FBML as defined in the *Domain ID* and *WWN* fields below the button.
- The Pending Fabric Binding Membership List—Enables you to view the pending FBML as it is being updated and to delete unattached members from the list. Members of the pending FBML are listed by WWN.

**NOTE:** For detailed instructions on configuring fabric binding, review the *SANpilot User Manual*.

---

## Subtask Q: Enable or Disable Enterprise Fabric Mode

Perform this procedure to toggle (enable or disable) the use of Enterprise Fabric Mode (EFM). The SANtegrity feature must be installed to access this control ([Subtask S: Install Feature Keys](#) on page 2-111). If the feature is not installed, the message **This Feature Not Installed** appears.

To enable or disable EFM:

1. At the *Configure* panel, click the *EFM* tab. The *Security* page displays with the *EFM* tab selected (Figure 2-79).
2. Perform one of the following steps as required:
  - Click *Enable* to activate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.
  - Click *Disable* to deactivate EFM. The message **Your changes to enterprise fabric mode have been successfully activated** appears.

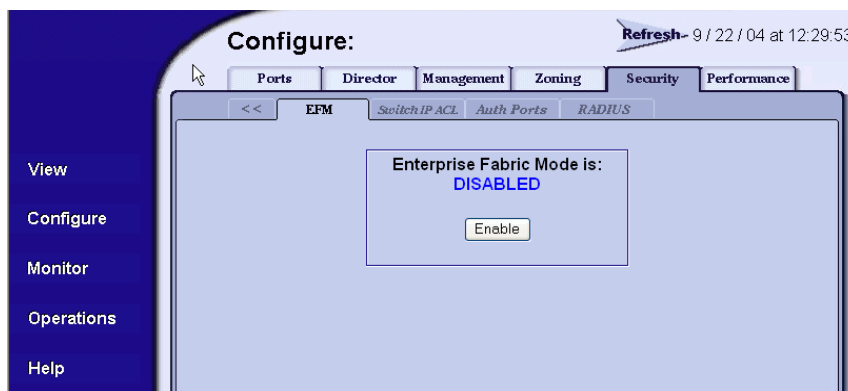


Figure 2-79 Configure Panel (Security Page with EFM Tab)

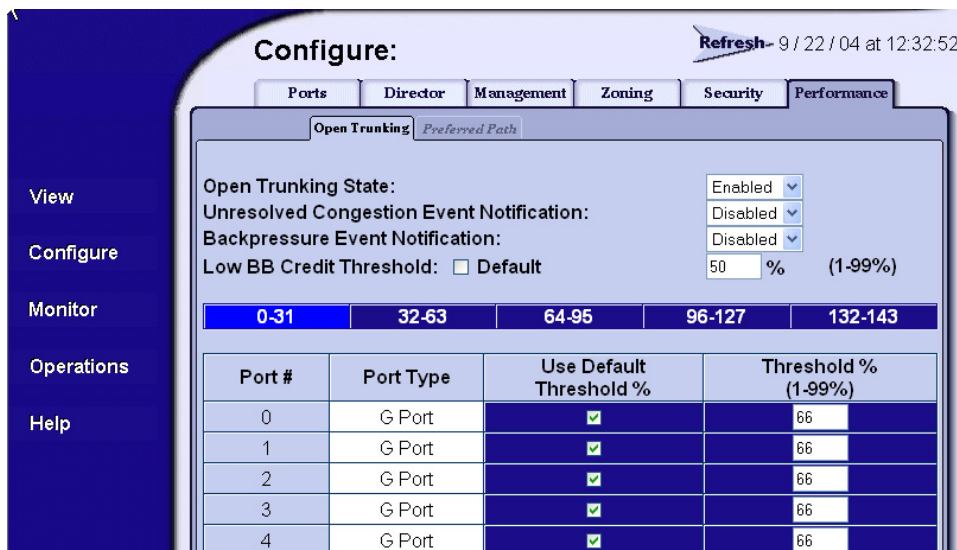
**NOTE:** For detailed information on configuring Enterprise Fabric Mode, review the *SANpilot User Manual*.

## Subtask R: Configure OpenTrunking

Perform this procedure to configure OpenTrunking parameters. The OpenTrunking feature must be installed to access this control ([Subtask S: Install Feature Keys](#) on page 2-111). If the feature is not installed, the message **OpenTrunking Feature Not Installed** appears.

To configure OpenTrunking parameters:

1. At the *Configure* panel, click the *Performance* tab. The *Performance* page displays with the *OpenTrunking* tab selected (Figure 2-80).



**Figure 2-80 Configure Panel (Performance Page with OpenTrunking Tab)**

- At the *OpenTrunking State* field, select *Enabled* or *Disabled*. When this parameter is enabled, the optional OpenTrunking feature is functional.
- At the *Unresolved Congestion Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, unresolved congestion events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

An unresolved congestion event occurs for a low-BB\_Credit ISL when the director firmware rerouting algorithm cannot route data flow to an alternate path (because doing so would exceed the alternate path low BB\_Credit threshold).

- At the *Backpressure Event Notification* field, select *Enabled* or *Disabled*. When this parameter is enabled, backpressure events are recorded in the event log, and SNMP trap messages are generated and transmitted (if SNMP is configured).

A backpressure event occurs when the percent time an ISL has low BB\_Credit exceeds the low BB\_Credit threshold.

- d. The low BB\_Credit threshold is the percent time an ISL is allowed to not transmit data because BB\_Credit is unavailable. When the threshold is exceeded, data is rerouted to another ISL. In addition, traffic cannot be rerouted to another low-threshold ISL. Use one of the following to set the low BB\_Credit threshold:
  - Click the *Default* check box. A check mark appears in the box and a calculated default value appears (1% to 99%) in the *Low BB\_Credit Threshold* field. If the default is enabled, a value cannot be entered in the *Low BB\_Credit Threshold* field.
  - Ensure the *Default* check box is blank. At the *Low BB\_Credit Threshold* field, type a percentage value from 1% to 99%.

---

**NOTE:** The default low BB\_Credit threshold is calculated by the director firmware.

---

2. For each director port:
  - a. Click the check box in the *Default Threshold %* column. A check mark appears in the box and a calculated default value appears (1% to 99%) in the associated field in the *Threshold %* column. If the default is enabled, a value cannot be entered in the *Threshold %* column.
  - b. Ensure the check box in the *Default Threshold %* column is blank. At the associated field in the *Threshold %* column, type a percentage value from 1% to 99%.

---

**NOTE:** The default low BB\_Credit threshold is calculated by the director firmware.

---

3. Click *Activate* to save the information. The message **Your changes to the port binding configuration have been successfully activated** appears.
4. If additional optional features will be installed, go to [Subtask S: Install Feature Keys](#) following. If no feature keys will be installed, go to [Task 12: Cable Fibre Channel Ports](#) on page 2-113.

---

## Subtask S: Install Feature Keys

Perform this procedure to view a list of installed features install one or more optional features.

A feature key is an alphanumeric string consisting of uppercase and lowercase characters. The number of characters may vary. The feature key is case sensitive and must be entered exactly, including dashes.

The following is an example of a feature key format:

**XxXx-XXxX-xxXX-xX.**

---

**NOTE:** You must be logged in as an Administrator-level rights to install feature keys.

---

After obtaining the feature key, install the feature.

1. Set the director offline.
  - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Director* page displays with the *Beacon* tab selected
  - b. Click the *Online State* tab, then click *Set Offline*. The message **Your operations changes have been successfully activated** appears.
2. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Director* page displayed.
3. Click the *Feature Installation* tab. The *Operations* panel opens with the *Feature Installation* page displayed ([Figure 2-81](#)).



**Figure 2-81 Operations Panel (Feature Installation Tab)**

4. Type the feature key and click *Activate*. The interface displays a confirmation page with a warning, stating this action overrides the current set of director features.
5. Click *Activate* to activate the new feature key. The director performs an IPL when the feature key is activated.

---

**NOTE:** When *Activate* is selected, all current features are replaced with new features. Features not included in the new feature key are no longer available on the system. Because of this, it is important to verify that the feature key enables all of designed features.

---

6. Set the director online:
  - a. At the *Configure* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens and the *Switch* page displays with the *Beacon* tab selected
  - b. Click the *Online State* tab, then click *Set Online*. The message **Your operations changes have been successfully activated** appears.

---

**NOTE:** PFE keys are encoded to work only with the serial number of the installed director. Record the key to re-install the feature. If the director must be replaced, obtain new PFE keys from the McDATA Solution Center (800-752-4572 or [support@mcddata.com](mailto:support@mcddata.com)). Have the serial numbers of the old and new directors, and the old PFE key number or transaction code available.

---

---

**NOTE:** If you receive the error message 238, either the feature key was entered incorrectly or the feature key is not valid for that feature. Contact the McDATA Solution Center for assistance.

---

---

## Task 12: Cable Fibre Channel Ports

Perform this task to connect devices to the director. To cable Fibre Channel ports:

1. Route singlemode or multimode fiber-optic cables (depending on the type of SFP optic transceivers installed) from customer-specified devices to ports at the front of the director.
2. Connect device cables to ports and route the cables through the cable management assembly at the bottom front of the director. Start with the center port cards adjacent to the CTP cards and work outward. In addition, start with the bottom port of each port card and work upward.
3. Perform one of the following:
  - If the director is installed on a table or desk top, bundle and secure the Fibre Channel cables as directed by the customer.
  - If the director is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the director and other equipment (groups of 16 maximum), and secure them as directed by the customer.
  - If the director is installed in a McDATA Fabriccenter equipment cabinet, bundle Fibre Channel cables from the director and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.
4. Set the director online (*Set the Director Online or Offline* on page 4-43).

---

## Task 13: Configure Zoning

Perform this procedure to:

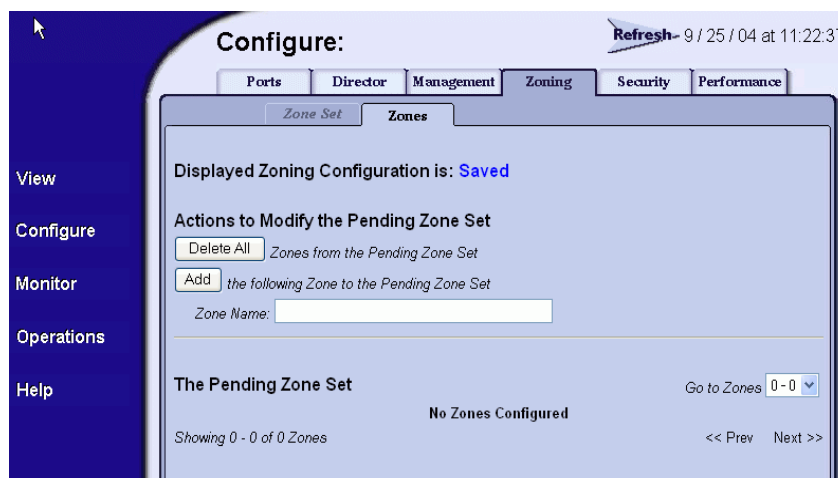
- Configure, change, add, or delete zones. A zone is a group of devices that can access each other through port- to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.

- Configure, change, enable, or disable zone sets. A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single director or a multiswitch fabric. Only one zone set can be active at one time.
5. If the installation is being performed from the SANpilot interface, go to [Configure Zones \(SANpilot Interface\)](#) following. If the installation is being performed from the management server, zoning is configured on a fabric-wide basis through the SAN management application. Refer to the *McDATA Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153), *McDATA Enterprise Fabric Connectivity Manager User Manual* (620-005001), or *SANavigator User Guide* (621-000013).

## Configure Zones (SANpilot Interface)

To configure zones at the SANpilot interface:

1. At the *Configure* panel, click the *Zoning* tab. The *Zoning* page displays with the *Zone Set* tab selected. Click the *Zones* tab. The *Zoning* page displays with the *Zones* tab selected ([Figure 2-82](#)).



**Figure 2-82 Configure Panel (Zoning Page with Zones Tab)**

2. To configure a zone, add the zone name to the zoning library. The following naming conventions apply to zones and zone sets:



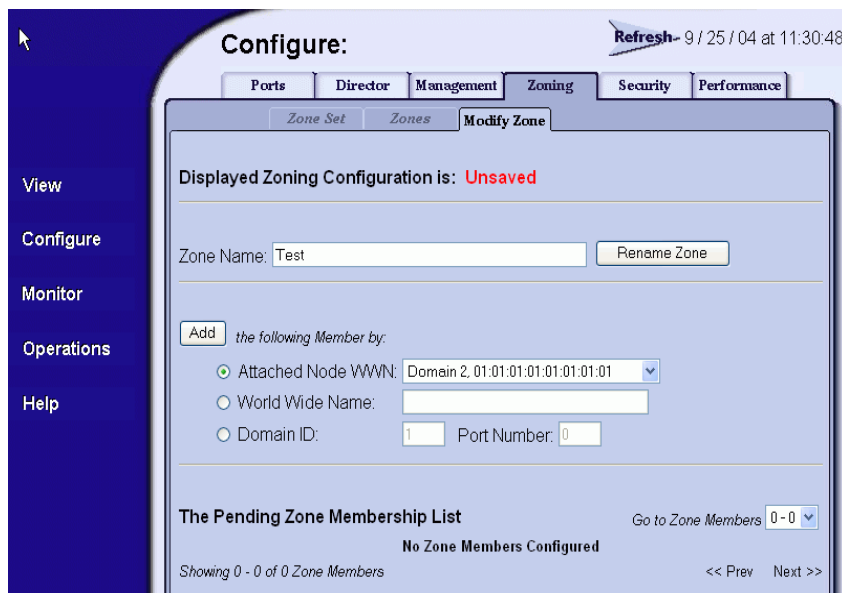
- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (A through Z or a through z).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret ( ^ ), hyphen ( - ), underscore ( \_ ), or dollar ( \$ ) symbols.
- A zone set name can have a maximum of 64 characters.

---

**NOTE:** A director can have at most 1024 zones.

---

3. Type the zone name and click *Add New Zone*. After the name is validated, the new zone name (**Zone-1**) and an associated *Delete* button appear at the bottom of the page. Note the following:
  - **Save and activate the zone** - Changes to a zone or zoning configuration are not saved and activated on the director or switch until saved as part of a zone set ([Configure Zone Sets \(SANpilot Interface\)](#) on page 2-117).
  - **Delete all zones** - To delete all configured zones and zone members, click *Delete All Zones*. A confirmation dialog box displays. Click *OK* to delete all zones.
  - **Delete a single zone** - To delete a single zone and its zone members, click the *Delete* button adjacent to the zone name. A confirmation dialog box displays. Click *OK* to delete the zone.
  - **Go to Zones** - If a zone set contains more than 64 zones, the *Go to Zones* link activates to display subsequent pages.
4. To add devices (members) to the zone, click the zone name (**Zone-1**). The *Zoning* page displays with the *Modify Zone* tab selected ([Figure 2-83](#)).



**Figure 2-83 Configure Panel (Zoning Page with Modify Zone Tab)**

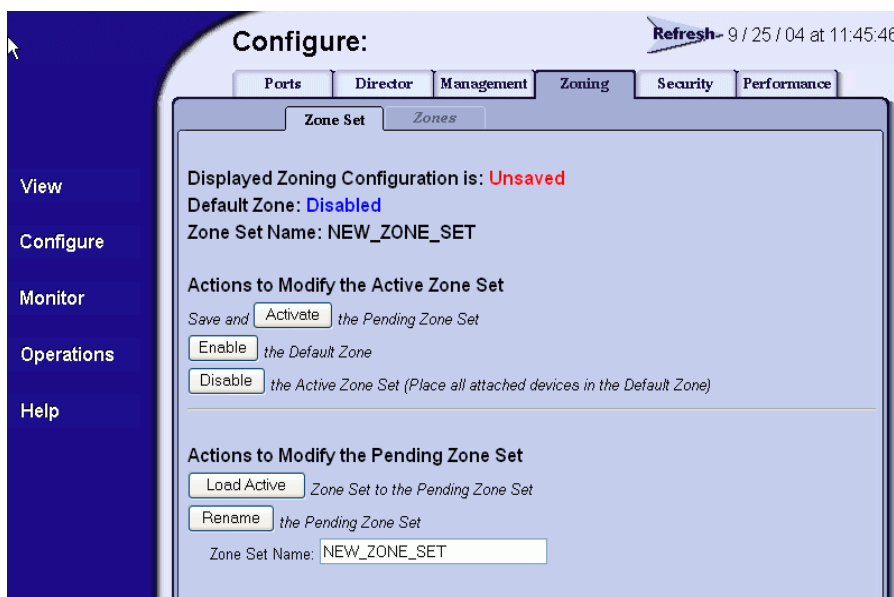
5. To rename a configured zone, type the new name in the *Zone* field and click *Rename Zone*. After the name is validated, the zone name is changed.
6. Add or delete zone members.
  - **Add member by attached node WWN** - Select the WWN of an attached device (node) from the *Attached Node World Wide Name* drop-down list and click the adjacent *Add Member* button. The device is added to the zone.
  - **Add member by WWN** - Type the WWN of an attached device in the *World Wide Name* field and click the adjacent *Add Member* button. The device is added to the zone.
  - **Add member by domain ID and port number** - Type the domain ID (1 through 31) of the director or switch in the *Domain ID* field, type the director port number to which a device is attached, and click the adjacent *Add Member* button. The device attached to that port is added to the zone.

7. Changes to a zone, zoning configuration, or zone member are not saved and activated on the director until saved as part of a zone set. Go to [Configure Zone Sets \(SANpilot Interface\)](#) following to perform this function.

## Configure Zone Sets (SANpilot Interface)

To configure zone sets at the SANpilot interface:

1. At the *Configure* panel and *Zoning* page, click the *Zone Set* tab. The *Zoning* page displays with the *Zone Set* tab selected ([Figure 2-84](#)).



**Figure 2-84 Configure Panel (Zoning Page with Zone Set Tab)**

2. To create a zone set that incorporates zones and zone members (configured under [Configure Zones \(SANpilot Interface\)](#) on page 2-114), type a new zone set name in the *Zone Set Name* field.
3. Click *Save and Activate Zoning Configuration*. After the zone set name is validated, a confirmation dialog box displays.
4. Click *OK* to save and activate the new zone set. The message **Your changes to the Zoning configuration have been successfully activated** appears. Note the following:

- **Rename the pending zone set** - To rename a zone set, type the new name in the *Zone Set Name* field. Click *Rename Zone Set*. The new zone set name is validated and changed.
- **Enable or disable default zone** - To toggle (enable or disable) the default zone state, click *Enable Default Zone* or *Disable Default Zone*. Depending on the toggle state, the *Default Zone* field changes to **Enabled** or **Disabled**.
- **Disable zone set** - To disable the active zone set and place all attached devices in the default zone, click *Disable Zone Set*. A confirmation dialog box displays. Click OK to disable the active zone set.
- **Discard changes** - To discard unsaved changes made to a zone set configuration and revert to a saved zoning configuration, click *Discard Changes*. A confirmation dialog box displays. Click OK to discard the changes.

## Task 14: Connect the Director to a Fabric Element

Connect the director to an expansion port (E\_Port) of a fabric element (director or switch) to provide fabric-attached Fibre channel connectivity.

To connect the director to a fabric element and create an ISL:

1. Ensure the fabric element is defined to the SAN management application or accessible by the SANpilot interface. If the fabric element must be defined, refer to the director or switch installation manual for instructions.
2. Ensure the preferred domain ID for the director is unique and does not conflict with the ID of another director or switch participating in the fabric.
  - If the domain ID must be changed from the management server, see [Task 8: Configure the Director at the Element Manager Application](#) on page 2-49.
  - If the domain ID must be changed from the SANpilot interface, see [Task 11: Configure the Director at the SANpilot Interface](#) on page 2-80.
3. Ensure the R\_A\_TOV and E\_D\_TOV values for the Intrepid 6140 Director are identical to the values for all directors or switches in the fabric.

- If the values must be changed from the management server, see [Task 8: Configure the Director at the Element Manager Application](#) on page 2-49.
  - If the values must be changed from the SANpilot interface, see [Task 11: Configure the Director at the SANpilot Interface](#) on page 2-80.
4. Route a multimode or singlemode fiber-optic cable (depending on the type of transceiver installed) from a customer-specified E\_Port of the fabric element to the director.
  5. If the director is managed by a management server, go to [step 6](#). If the director is managed by the SANpilot interface:
    - a. At the *Configure* panel, select the *View* option at the left side of the panel. The *View* panel opens with the *Director* page displayed.
    - b. Double-click the graphical port connector used for the fabric ISL.
    - c. The *View* panel opens with the *Port Properties* page displayed. Port properties appear for the selected port.
    - d. Ensure the *Operational State* field displays **Online** and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem. If no problems are indicated, installation tasks are complete.
  6. At the SAN management application physical map, right-click the director icon, then select *Element Manager* from the pop-up menu.
  7. If required, click the *Hardware* tab. The *Hardware View* displays.
  8. Double-click the graphical port connector used for the fabric ISL. The *Port Properties* dialog box displays ([Figure 2-85](#)).
  9. Ensure the *Link Incident* field displays **None** and the *Reason* field is blank. If an ISL segmentation or other problem is indicated, go to [Chapter 3, Maintenance Analysis Procedures \(MAPS\)](#) to isolate the problem.

Port Number	2
Port Name	
Type	F_Port
Operating Speed	1 Gig
Port WWN	McDATA-20:06:08:00:88:00:21:00
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	

Close Help

Figure 2-85 Port Properties Dialog Box

## Task 15: Register with the McDATA File Center

To complete the installation, register with the McDATA File Center web site to receive e-mail updates and access the following:

- Technical publications.
- Firmware and software upgrades.
- Technical newsletters.
- Release notes.

To register with the McDATA File Center:

1. At a PC with Internet access, open the McDATA File Center home page ([Figure 2-86](#)). The uniform resource locator (URL) is <http://central.mcddata.com>.

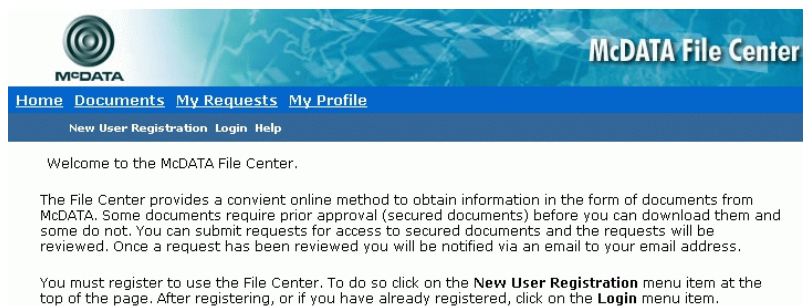


Figure 2-86 McDATA File Center Home Page

2. Click the *New User Registration* option at the top of the home page. The File Center *New User Registration* page displays (Figure 2-87). Use the registration page to input required and optional user information. The following information is required:
  - Password.
  - Verify password.
  - First name.
  - Last name.
  - E-mail address.
  - Company.
  - Title.
3. Complete the information fields and click *Register*. The registration is complete and File Center login information is transmitted to the e-mail address specified on the *New User Registration* page.
4. At the browser PC, close the Internet session. If no director problems are indicated, installation tasks are complete.

[New User Registration](#) [Login](#) [Help](#)

Registration: New File Center

Below are a few fields we need you to fill in so that we can better fulfill your request for information. You will only have to do this once and the information will not be released to any other companies. Information requested below will assist us in routing your request to the appropriate SAN Professional.

**There are some mandatory fields that have not been filled in yet or are invalid. Please correct them and click the Register button. Field specific errors are shown to the right of the fields.**

Basic User Information

In this section we need to collect some basic information about you and how we can contact you.

Password:	<input type="password"/>	Password is required.
Verify Password:	<input type="password"/>	Verify Password is required.
First Name:	<input type="text"/>	First Name is required.
Middle Name:	<input type="text"/>	
Last Name:	<input type="text"/>	Last Name is required.
E-mail Address:	<input type="text"/>	E-mail Address is required.
Company:	<input type="text"/>	Company is required.
Title:	<input type="text"/>	Title is required.
Phone Number:	<input type="text"/>	
Fax Number:	<input type="text"/>	

Register

Figure 2-87 McDATA File Center (New User Registration Page)



## Maintenance Analysis Procedures (MAPS)

This chapter describes diagnostic procedures used by service representatives to fault isolate Intrepid 6140 Director problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

### Maintenance Analysis Procedures

**NOTE:** The screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The MAPs provide fault isolation and related service procedures. The procedures vary depending on the diagnostic information provided. MAPs are step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system events, isolate a director failure to a single FRU, remove and replace the failed FRU, and verify director operation.

## Factory Defaults

[Table 3-1](#) lists factory-set defaults for the Intrepid 6140 Director passwords (customer and maintenance-level), and the director Internet Protocol (IP) address, subnet mask, and gateway address.

**Table 3-1 Factory-Set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Quick Start

[Table 3-2](#) lists the MAPs. Fault isolation normally begins at [MAP 0000: Start MAP](#) on page 3-9.

However, [Table 3-3](#) lists the event codes and the corresponding MAPs. It is a quick start, if an event code is readily available.

**Table 3-2 MAP Summary**

MAP	Page
MAP 0000: Start MAP	<a href="#">3-9</a>
MAP 0100: Power Distribution Analysis	<a href="#">3-33</a>
MAP 0200: POST Failure Analysis	<a href="#">3-42</a>
MAP 0300: Server Application Problem Determination	<a href="#">3-47</a>
MAP 0400: Loss of Server Communication	<a href="#">3-56</a>
MAP 0500: FRU Failure Analysis	<a href="#">3-74</a>
MAP 0600: Port Card Failure and Link Incident Analysis	<a href="#">3-82</a>
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	<a href="#">3-104</a>
MAP 0800: Server Hardware Problem Determination	<a href="#">3-121</a>

**Table 3-3 Event Codes versus Maintenance Action**

Event Code	Explanation	Action
001	System power-down.	Power on director.
010	Login server unable to synchronize databases.	Go to <a href="#">MAP 0700</a> .
011	Login server database invalid.	Go to <a href="#">MAP 0700</a> .
020	Name server unable to synchronize databases.	Go to <a href="#">MAP 0700</a> .
021	Name server database invalid.	Go to <a href="#">MAP 0700</a> .
031	SNMP request received from unauthorized community.	Add community name through the Element Manager application.
050	Management server unable to synchronize databases.	Go to <a href="#">MAP 0700</a> .
051	Management server database invalid.	Go to <a href="#">MAP 0700</a> .
052	Management server internal error.	Go to <a href="#">MAP 0700</a> .
060	Fabric controller unable to synchronize databases.	Go to <a href="#">MAP 0700</a> .
061	Fabric controller database invalid.	Go to <a href="#">MAP 0700</a> .
062	Maximum interswitch hop count exceeded.	Go to <a href="#">MAP 0700</a> .
063	Remote director or switch has too many ISLs.	Go to <a href="#">MAP 0700</a> .
070	E_Port is segmented.	Go to <a href="#">MAP 0700</a> .
071	Director is isolated.	Go to <a href="#">MAP 0700</a> .
072	E_Port connected to unsupported switch.	Go to <a href="#">MAP 0700</a> .
073	Fabric initialization error.	Event data intended for engineering evaluation. Perform data collection procedure ( <a href="#">Collecting Maintenance Data on page 4–39</a> ) and return CD to McDATA support personnel.

Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
074	ILS frame delivery error threshold exceeded.	Event data intended for engineering evaluation. Perform data collection procedure ( <i>Collecting Maintenance Data on page 4–39</i> ) and return CD to McDATA support personnel.
080	Unauthorized worldwide name.	Go to <b>MAP 0600</b> .
081	Invalid attachment.	Go to <b>MAP 0600</b> .
090	Database replication time out.	Event data intended for engineering evaluation. Perform data collection procedure ( <i>Collecting Maintenance Data on page 4–39</i> ) and return CD to McDATA support personnel.
091	Database replication discontinued.	If this event occurs without the backup CTP failing or being removed, perform data collection procedure ( <i>Collecting Maintenance Data on page 4–39</i> ) and return CD to McDATA support personnel. Otherwise no action required.
120	Error while processing system management command.	If this event persists, perform data collection procedure ( <i>Collecting Maintenance Data on page 4–39</i> ) and return CD to McDATA support personnel.

Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to <a href="#">MAP 0700</a> .
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to <a href="#">MAP 0700</a> .
143	Low BB_Credit relieved on an ISL.	No action required.
150	Zone merge failure.	Go to <a href="#">MAP 0700</a> .
151	Fabric configuration failure.	If this event persists, perform data collection procedure ( <a href="#">Collecting Maintenance Data</a> on page 4-39) and return CD to McDATA support personnel.
200	Power supply AC voltage failure.	Go to <a href="#">MAP 0100</a> .
201	Power supply DC voltage failure.	Go to <a href="#">MAP 0100</a> .
202	Power supply thermal failure.	Go to <a href="#">MAP 0100</a> .
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
208	Power supply false shutdown.	Go to <a href="#">MAP 0100</a> .
300	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .
301	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .
302	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .
303	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .
304	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .
305	Cooling fan propeller failed.	Go to <a href="#">MAP 0500</a> .

Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
320	Fan module removed.	Replace FRU.
321	Fan module installed.	No action required.
400	Power-up diagnostic failure.	Go to <a href="#">MAP 0200</a> .
410	CTP card reset.	No action required.
411	Firmware fault.	Go to <a href="#">MAP 0200</a> .
412	CTP watchdog timer reset.	Go to <a href="#">Collecting Maintenance Data</a> on page 4-39.
413	Backup CTP card POST failure.	Go to <a href="#">MAP 0200</a> .
414	Backup CTP card failed.	Go to <a href="#">MAP 0500</a> .
415	Backup CTP card removed.	Replace FRU.
416	Backup CTP card installed.	No action required.
417	CTP card firmware synchronization initiated.	No action required.
418	User-initiated CTP card switchover.	No action required.
420	Backup CTP card NV-RAM failure.	Go to <a href="#">MAP 0500</a> .
421	Firmware download complete.	No action required.
422	CTP firmware synchronization complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to <a href="#">MAP 0500</a> .
430	Excessive Ethernet transmit errors.	Go to <a href="#">MAP 0400</a> .

Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
431	Excessive Ethernet receive errors.	Go to <a href="#">MAP 0400</a> .
432	Ethernet adapter reset.	Go to <a href="#">MAP 0400</a> .
433	Non-recoverable Ethernet fault.	Go to <a href="#">MAP 0500</a> .
440	Embedded port hardware failed.	Go to <a href="#">MAP 0500</a> .
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
450	Serial number mismatch detected.	No action required.
451	Switch speed incompatibility detected.	No action required.
452	Backup CTP incompatible with configured system settings.	Replace backup CTP card with a card that is capable of supporting the configured settings, or adjust the settings to be compatible with the backup CTP card.
453	New feature key installed.	No action required.
500	Port card hot-insertion initiated.	No action required.
501	Port card recognized.	No action required.
502	Port module anomaly detected.	No action required.
503	Port card hot-removal completed.	No action required.
504	Port module card failure.	Go to <a href="#">MAP 0600</a> .
505	Port module revision not supported.	Go to <a href="#">MAP 0600</a> .
506	Fibre Channel port failure.	Go to <a href="#">MAP 0600</a> .
507	Loopback diagnostics port failure.	Go to <a href="#">MAP 0600</a> .
508	Fibre Channel port anomaly detected.	No action required.
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to <a href="#">MAP 0600</a> .

Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to <a href="#">MAP 0600</a> .
581	Implicit incident.	Go to <a href="#">MAP 0600</a> .
582	Bit error threshold exceeded.	Go to <a href="#">MAP 0600</a> .
583	Loss of signal or loss of synchronization.	Go to <a href="#">MAP 0600</a> .
584	Not operational primitive sequence received.	Go to <a href="#">MAP 0600</a> .
585	Primitive sequence timeout.	Go to <a href="#">MAP 0600</a> .
586	Invalid primitive sequence received for current link state.	Go to <a href="#">MAP 0600</a> .
600	SBAR assembly hot-insertion initiated.	No action required.
601	SBAR assembly recognized.	No action required.
602	SBAR assembly anomaly detected.	No action required.
603	SBAR assembly hot-removal completed.	No action required.
604	SBAR assembly failure.	Go to <a href="#">MAP 0500</a> .
605	SBAR assembly revision not supported.	Go to <a href="#">MAP 0500</a> .
607	Director contains no operational SBAR assemblies.	Go to <a href="#">MAP 0500</a> .
608	User initiated SBAR switch-over.	No action required.
620	SBAR fan failure.	Go to <a href="#">MAP 0500</a> .
621	Failed SBAR fan recovered.	No action required.
800	High temperature warning (port module thermal sensor).	Go to <a href="#">MAP 0600</a> .
801	Critically hot temperature warning (port module thermal sensor).	Go to <a href="#">MAP 0600</a> .
802	Port module shutdown due to thermal violation.	Go to <a href="#">MAP 0600</a> .
805	High temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">MAP 0500</a> .



Table 3-3 Event Codes versus Maintenance Action (*continued*)

Event Code	Explanation	Action
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">MAP 0500</a> .
807	SBAR assembly shutdown due to thermal violation.	Go to <a href="#">MAP 0500</a> .
810	High temperature warning (CTP card thermal sensor).	Go to <a href="#">MAP 0500</a> .
811	Critically hot temperature warning (CTP card thermal sensor).	Go to <a href="#">MAP 0500</a> .
812	CTP card shutdown due to thermal violation.	Go to <a href="#">MAP 0500</a> .
850	System shutdown due to CTP card thermal violations.	Go to <a href="#">MAP 0500</a> .

## MAP 0000: Start MAP

This MAP describes initial fault isolation for the Intrepid 6140 Director. Fault isolation begins at the management server, Internet-connected PC accessing the SANpilot interface, customer-supplied server running the EFCM Lite application, failed director, or director-attached host.

### 1

Prior to fault isolation, acquire the following information from the customer:

- A system configuration drawing or planning worksheet that includes the management server, customer-supplied server (accessing the SANpilot interface or running the EFCM Lite application), directors and switches, other McDATA products, and device connections.
- The location of the management server or customer-supplied server and all directors or switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the director reporting the problem.
- If performing fault isolation using the management server:

- The Windows 2000 user name and password. These are required when prompted during any MAP or repair procedure that directs the management server to be rebooted.
- The user name, maintenance password, and management server name. All are case sensitive and required when prompted at the *EFCM Log In* or *SANavigator Log In* dialog box.
- If performing fault isolation using a customer-supplied server accessing the SANpilot interface, the administrator user name and password. Both are case sensitive and required when prompted at the *Username and Password Required* dialog box.
- If performing fault isolation using a customer-supplied server running the EFCM Lite application:
  - The operating system user name and password. These are required when prompted during any MAP or repair procedure that directs the server to be rebooted.
  - The user name, maintenance password, and server name. All are case sensitive and required when prompted at the *EFCM Log In* dialog box.

**Continue.**

## 2

Are you at the management server or customer-supplied server running the EFCM Lite application?

**YES    NO**



**Go to [step 24](#)**

## 3

Did the management server or customer-supplied server lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a *Dr. Watson for Windows 2000* dialog box?

**NO    YES**



A management server or customer-supplied server application problem is indicated. Event codes are not

recorded. Go to [MAP 0300: Server Application Problem Determination](#) on page 3-47. **Exit MAP.**

#### 4

Did the management server or customer-supplied server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

**NO YES**



A management server or customer-supplied server application problem is indicated. Event codes are not recorded. Go to [MAP 0300: Server Application Problem Determination](#) on page 3-47. **Exit MAP.**

#### 5

Is the SAN management application (EFCM or SANavigator) active?

**NO YES**



**Go to [step 7](#).**

#### 6

Reboot the management server or customer-supplied server. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays ([Figure 3-1](#)).



**Figure 3-1 Shut Down Windows Dialog Box**

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.

- c. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the server and perform power-on self-tests (POSTs). During POSTs:
  1. The green LCD panel illuminates.
  2. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  3. After a few seconds, the LCD panel displays the following message about the boot sequence selection ([Figure 3-2](#)):



Boot from LAN?  
Press <Enter>

**Figure 3-2 LCD Panel During Boot Sequence**

4. Ignore the message. After ten seconds, the server performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - Central processing unit (CPU) temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- e. After rebooting the server at the LCD panel, log on to the management server Windows 2000 desktop through a LAN connection to a browser-capable PC ([Access the Management Server Desktop](#) on page 2-26). The SAN management application start and the *EFCM Log In* or *SANavigator Log In* displays ([Figure 3-3](#)).



Connect to SANavigator server to open a SAN

Network Address: localhost [Delete]

Server Name: PCNEF0911-1

User ID: [ ]

Password: [ ]

☒ Forget password  
☐ Save password

[Login] [Exit]

Server Available

**Figure 3-3 EFCM Log In or SANavigator Log In Dialog Box**

- f. Type a user ID and password, and click *Login*. The SAN management application opens and the EFCM or SANavigator main window displays (Figure 3-4).

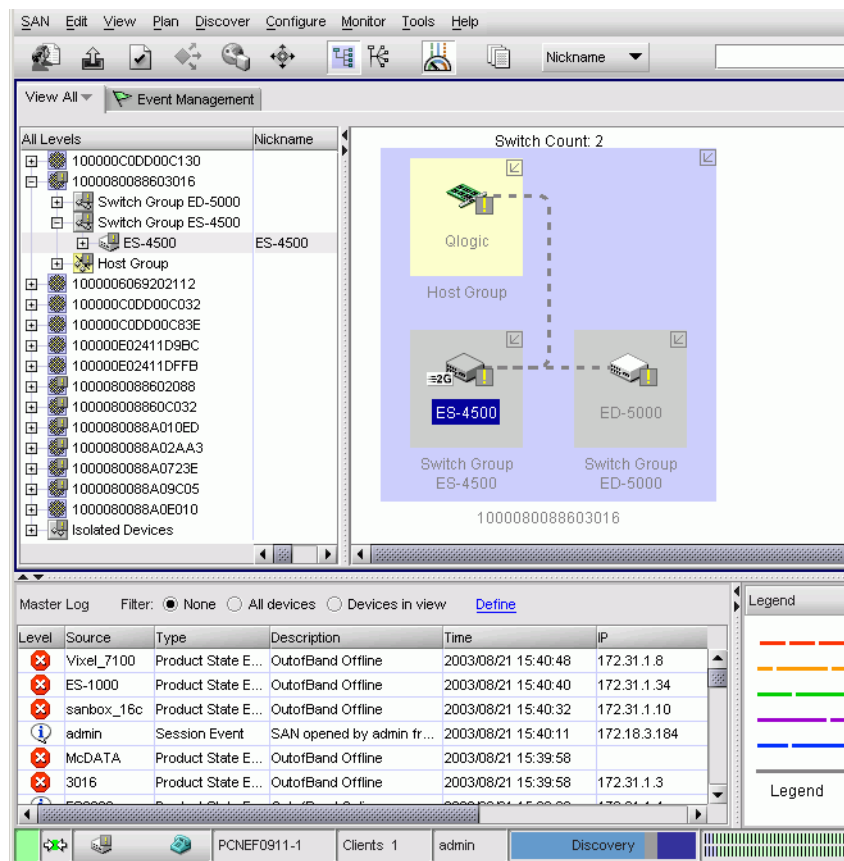


Figure 3-4 Main Window: Example (EFCM or SANavigator)

Did the main window display and does the SAN management application appear operational?

YES NO



A management server or customer-supplied server hardware problem is indicated. Event codes are not recorded. Go to [MAP 0800: Server Hardware Problem Determination](#) on page 3-121. **Exit MAP.**

7

Inspect the status symbol associated with the Intrepid 6140 Director at the main window physical map or product list. The symbol shows

the status of the director or the status of the link between the management server or customer-supplied server and the director:

- No status symbol indicates that the director is operational.
- A yellow triangle indicates that the director is operating in degraded mode.
- A red diamond indicates that the director is not operational.
- A grey square with yellow exclamation mark indicates that the status of the director is unknown.

Is a grey square with yellow exclamation mark associated with the icon representing the director reporting the problem?

**YES    NO**



**Go to [step 11](#).**

The status symbol indicates the management server or customer-supplied server cannot communicate with the director because:

- The director-to-server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director control processor (CTP) cards failed.

**Continue.**

## 8

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES    NO**



A power distribution problem is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 9

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

**NO      YES**



Failure of both CTP cards is indicated. Event codes are not recorded. Go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 10

A director-to-server Ethernet link failure is indicated.

**Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0400: Loss of Server Communication](#) on page 3-56.

**Exit MAP.**

## 11

Is a red diamond (failure indicator) associated with the icon representing the director reporting the problem?

**YES      NO**



**Go to step 14.**

## 12

Right-click the icon representing the director reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays.

At the *Hardware View*:

- Observe that the *Intrepid 6140 Status* table is yellow and the director status is **NOT OPERATIONAL**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Do blinking red and yellow diamonds overlay all port card graphics?

**NO      YES**



Failure of all installed port cards is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**



## 13

Blinking red and yellow diamonds overlay both serial crossbar (SBAR) assembly graphics or both fan module graphics.

Redundant FRU failures are indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 14

Is a yellow triangle (attention indicator) associated with the icon representing the director reporting the problem?

**YES NO**



**Go to step 18.**

## 15

Right-click the icon representing the director reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays. At the *Hardware View*:

- Observe that the *Intrepid 6140 Status* table is yellow and the director status is **Minor Failure** or **Redundant Failure**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a power supply graphic?

**NO YES**



A power supply failure is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 16

Does a blinking red and yellow diamond overlay a port card graphic?

**NO YES**



A port card failure is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

## 17

A blinking red and yellow diamond overlays a control processor (CTP) card, SBAR assembly, or fan module graphic.

A FRU failure is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 18

No colored status symbol is associated the icon representing the director reporting the problem. Although the director is operational, a minor problem may exist.

Right-click the icon representing the director reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays. At the *Hardware View*:

- Inspect CTP cards, SBAR assemblies, and fan modules for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect port cards for a yellow triangle (attention indicator) that overlays the port card graphic.

Does a yellow triangle overlay a CTP card, SBAR assembly, or fan module graphic?

**YES    NO**



**Go to step 20.**

## 19

Beaconing is enabled for the FRU.

- a. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.
- b. Disable FRU beaconing.
  1. At the *Hardware View*, right-click the FRU graphic. A pop-up menu appears.
  2. Click the *Enable Beaconing* option. The check mark disappears from the box adjacent to the option, and FRU beaconing is disabled.

Was FRU beaconing enabled because a FRU failure or degradation was suspected?

YES    NO  
↓    The director appears operational. **Exit MAP.**

Go to **step 2.**

20

Does a yellow triangle (attention indicator) overlay a port card graphic?

YES    NO  
↓    **Go to step 22.**

21

Inspect the port state and LED status for all port cards with an attention indicator.

- a. Double-click the port card to open the *Port Card View*. At the *Port Card View*, double-click the port graphic with the attention indicator. The *Port Properties* dialog box displays (Figure 3-5).
- b. Inspect the *Operational State* field.

Port Number	2
Port Name	
Type	F_Port
Operating Speed	1 Gig
Port WWN	McDATA-20:06:08:00:88:00:21:00
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	

Close

Help

Figure 3-5    Port Properties Dialog Box

Does the *Operational State* field display a **Segmented E\_Port** message?

**NO      YES**



Expansion port (E\_Port) segmentation is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to *MAP 0700: Fabric, ISL, and Segmented Port Problem Determination* on page 3-104. **Exit MAP.**

A message displays indicating a link incident problem. **Go to step 23** to obtain event codes. If no event codes are found, go to *MAP 0600: Port Card Failure and Link Incident Analysis* on page 3-82.

**Exit MAP.**

## 22

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the *Hardware View*, click *Logs* and select *Link Incident Log*. The *Link Incident Log* displays (Figure 3-6).

Date/Time ▲	port	Link Incident
2003/09/03 14:59:10	9	NOS Received
2003/09/03 14:59:04	11	NOS Received
2003/09/03 14:58:37	9	NOS Received

Export...
Clear
Refresh
Close
Help

**Figure 3-6** Link Incident Log

If a link incident occurred, the affected port number is listed with one of the following messages.

**Link interface incident - implicit incident.**

**Link interface incident - bit-error threshold exceeded.**

**Link failure - loss of signal or loss of synchronization.**

**Link failure - not-operational primitive sequence (NOS) received.**

**Link failure - primitive sequence timeout.**

**Link failure - invalid primitive sequence received for the current link state.**

Did one of the listed messages appear in the *Link Incident Log*?

YES NO

↓ The director appears operational. **Exit MAP.**

A link incident problem is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

23

Obtain event codes from the *Intrepid 6140 Event Log*.

**NOTE:** If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and sequence, and determine if the codes are related to the problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

- a. At the *Hardware View*, click *Logs* and select *Event Log*. The *Event Log* displays ([Figure 3-7](#)).
- b. Record the event code, date, time, and severity (*Informational*, *Minor*, *Major*, or *Severe*).
- c. Record all event codes that may relate to the reported problem.

Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

Export...

Clear

Refresh

Close

Help

Figure 3-7 Event Log

Were one or more event codes found?

NO YES

↓ **Go to Table 3-3 on page 3-3** to interpret event codes.

Return to the MAP step that sent you here.

24

Are you at the director reporting the problem?

YES NO



Go to [step 36](#).

## 25

Is the power LED (green) at the director front bezel illuminated?

NO YES



Go to [step 30](#).

## 26

Is the director connected to facility AC power and powered on?

NO YES



Go to [step 29](#).

## 27

Connect the director to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

YES NO



A power distribution problem is indicated. Go to [step 23](#) to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. Exit MAP.

## 28

Is the power LED (green) at the director front bezel illuminated?

NO YES



Go to [step 30](#).

A faulty power LED is indicated, but director and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the module must be removed and replaced ([RRP: Fan Module](#) on page 5-27). Exit MAP.

## 29

Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**

- ↓ A power distribution problem is indicated. **Go to step 23** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

A faulty power LED is indicated, but director and Fibre Channel port operation is not disrupted. The LED is connected to the circuitry in a fan module, and the module must be removed and replaced ([RRP: Fan Module](#) on page 5-27). **Exit MAP.**

## 30

Is the system error LED (amber) at the director front bezel blinking?

**YES NO**

- ↓ **Go to step 32.**

## 31

Unit beaconing is enabled for the director.

- a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
- b. Disable unit beaconing.
  1. At the *Hardware View*, right-click the front bezel graphic (away from a FRU). A pop-up menu appears.
  2. Click the *Enable Unit Beaconing* option. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because a director failure or degradation was suspected?

**YES NO**

↓ The director appears operational. **Exit MAP.**

**Go to [step 24](#).**

## 32

Is the system error LED (amber) at the director front bezel illuminated?

**YES NO**

↓ The director appears operational. Verify operation at the management server or customer-supplied server. **Go to [step 3](#).**

## 33

Check FRUs (port cards, CTP cards, SBAR assemblies, power supplies, and fan modules) for failure symptoms.

Is the amber LED at the top of a port card illuminated or are any amber LEDs associated with Fibre Channel ports illuminated?

**NO YES**

↓ A port card or Fibre Channel port failure is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

## 34

Is the amber LED on a CTP card, SBAR assembly, or fan module illuminated?

**NO YES**

↓ A FRU failure is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 35

Is the green **PWR OK** LED on a power supply extinguished?

**NO YES**

↓ A power supply failure is indicated. **Go to [step 23](#)** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

The director appears operational. **Exit MAP.**



**36**

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer), an Internet connection to the director reporting the problem, and communicating with the director through the SANpilot interface?.

**YES NO**



**Go to [step 53](#).**

**37**

Is the web browser PC powered on and communicating with the director through the Internet connection and SANpilot interface?

**NO YES**

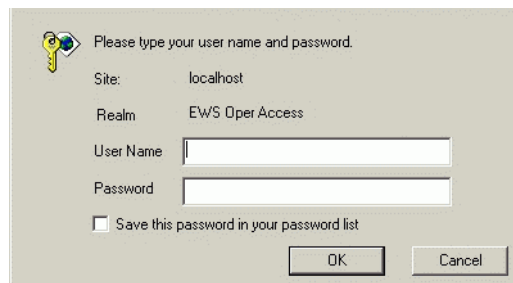


**Go to [step 39](#).**

**38**

Boot the web browser PC.

- a. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.
- b. Launch the PC browser application by double-clicking the Netscape Navigator icon or Internet Explorer icon at the Windows desktop.
- c. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the director. The *Username and Password Required* dialog box appears ([Figure 3-8](#)).



**Figure 3-8 Username and Password Required Dialog Box**

- d. Type the user name and password, and click **OK**. The SANpilot interface opens with the *View* panel displayed ([Figure 3-9](#)).

Continue.

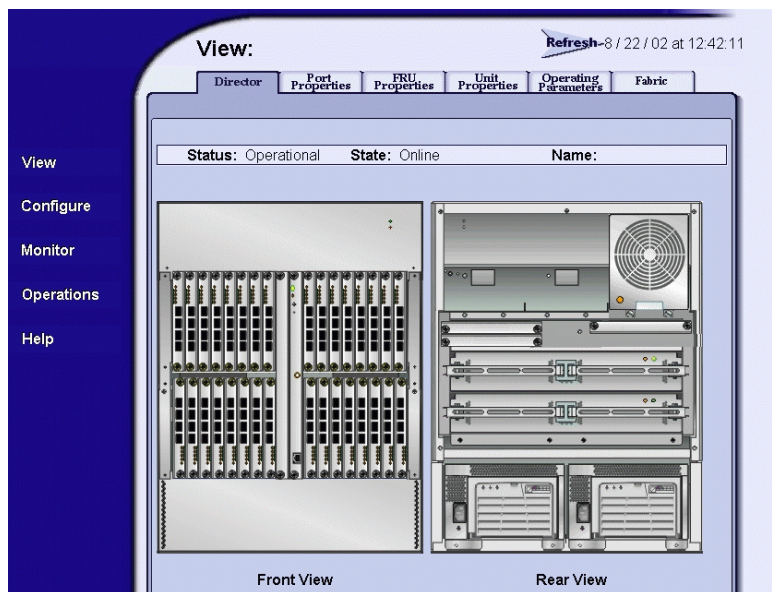


Figure 3-9 SANpilot Interface, View Panel

39

Does the SANpilot interface appear operational with the *View* panel displayed?

NO YES



Go to [step 44](#).

40

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

Continue.

## 41

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 42

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

**NO YES**

- ↓ Failure of both CTP cards is indicated. Event codes are not recorded. Go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 43

A director-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

- a. Wait approximately five minutes, then attempt to login to the director again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the director. The *Username and Password Required* dialog box appears.
- c. Type the user name and password, and click **OK**. If the *View* panel does not display, wait another five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

YES NO



Perform director fault isolation at the management server or customer-supplied server running the EFCM Lite application.  
**Go to step 3.**

## 44

At the *View* panel, inspect the *Status* field.

Does the director status indicate **Operational**?

NO YES



The director appears operational. **Exit MAP.**

## 45

Inspect Fibre Channel port operational states.

- At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays with port **0** highlighted (Figure 3-10).
- Inspect the *Beaconing* and *Operational State* fields.

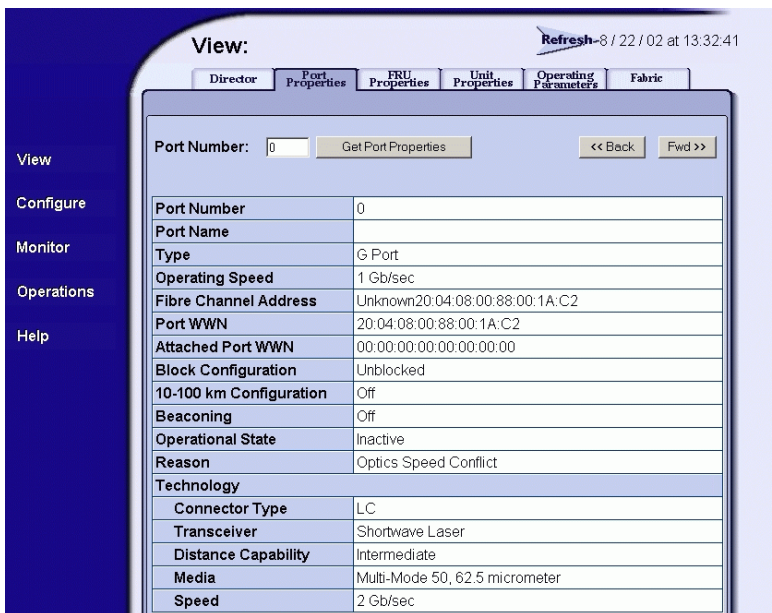


Figure 3-10 SANpilot Interface, View Panel

Does the *Beaconing* field display an **On** message?

YES NO



Go to [step 47](#).

## 46

Port beaconing is enabled.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing:
  1. At the *View* panel, select *Operations* at the left side of the panel. The *Operations* panel opens with the *Port Beaconing* page displayed.
  2. Click the *Beaconing State* check box for the port. The check mark disappears from the box and port beaconing is disabled.
  3. Return to the *View* panel (*Port Properties* tab).

**Continue.**

## 47

At the *View* panel, does the *Operational State* field display a **Segmented** message?

NO YES



Port segmentation is indicated. Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-104. **Exit MAP.**

## 48

At the *View* panel, does the *Operational State* field display a message indicating a port problem?

NO YES



Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

## 49

Repeat [step 45](#) through [step 48](#) for each remaining Fibre Channel port for which a problem is suspected (ports **1** through **139**).

Is an problem indicated for any of the ports?

NO YES



Go to [step 52](#) to obtain event codes. If no event codes are found, go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

## 50

Inspect power supply operational states.

- At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays ([Figure 3-11](#)).
- Inspect the *Status* fields for both power supplies.

FRU	Position	Status	Part Number	Serial Number
CTP	0	Active	470-000410-361	80341657
CTP	1	Backup	470-000410-361	80322136
SBAR	0	Active	002-002259-100	20460042
SBAR	1	Backup	002-002259-100	81160560
Power	0	Active	721-000042-001	Z59001930
Power	1	Active	721-000042-001	Z59001929
Fan	0	Active		
Fan	1	Active		
Backplane	0	Active	470-000418-202	20430519
Not Installed	0			
Not Installed	1			
Not Installed	2			
Not Installed	3			
GSF1	4	Active	470-000439-004	80430387
Not Installed	5			
Not Installed	6			
Not Installed	7			
Not Installed	8			
Not Installed	9			
Not Installed	10			
Not Installed	11			
GSF1	12	Active	470-000439-004	80430551
Not Installed	13			
GSF1	14	Active	470-000439-004	80430336
GSF1	15	Active	470-000439-004	80430296

Figure 3-11 SANpilot Interface, View Panel

Does the *Status* field display a **Failed** message for either power supply?

**NO      YES**



A power supply failure is indicated. **Go to step 52** to obtain event codes. If no event codes are found, go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 51

Inspect the *Status* fields for director FRUs, including CTP cards, SBAR assemblies, fan modules, and the backplane.

Does the *State* field display a **Failed** message for any of the FRUs?

**YES      NO**



The director appears operational. **Exit MAP.**

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 52

Obtain event codes from the SANpilot event log.

---

**NOTE:** If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and sequence, and determine if the codes are related to the problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

---

- a. At the *View* panel, select *Monitor* at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed.
- b. At the *Monitor* panel, click the *Log* tab. The *Monitor* panel (*Log* tab) displays ([Figure 3-12](#)).
- c. Record the event code, date, time, and severity (*Informational*, *Minor*, *Major*, or *Severe*).
- d. Record all event codes that may relate to the reported problem.

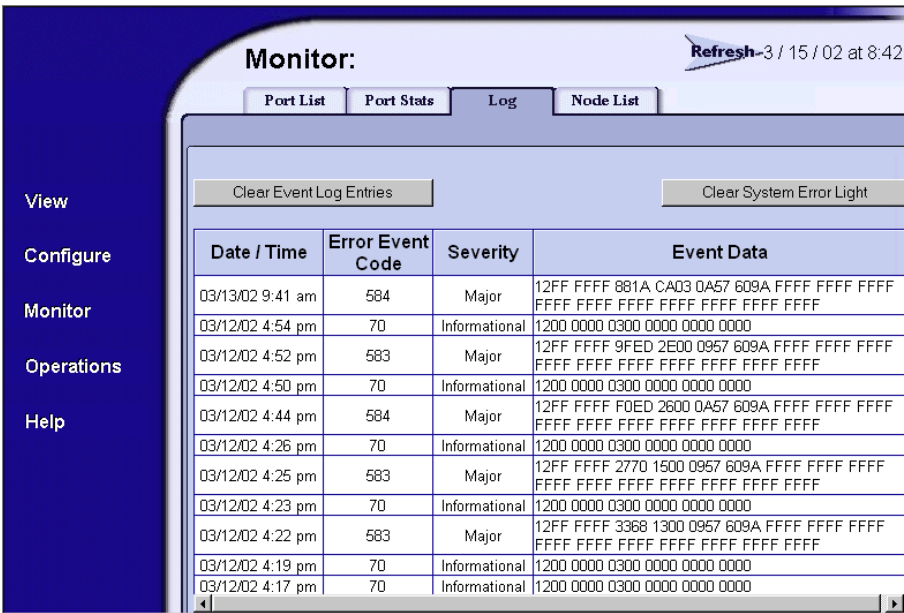


Figure 3-12 SANpilot Interface, Monitor Panel

Were one or more event codes found?

**NO YES**

↓ **Go to Table 3-3 on page 3-3 to interpret event codes.**

Return to the MAP step that sent you here.

**53**

You are at the console of an open systems interconnection (OSI) or Fibre Connection (FICON) server attached to the director reporting the problem. If an incident occurs on the Fibre Channel link between the director and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON).

Was a link incident record generated and sent to the director-attached OSI or FICON server?

**YES NO**

↓ **Perform director fault isolation at the management server or customer-supplied server running the EFCM Lite application. Go to step 3.**



## 54

The link incident record provides the attached director port numbers and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

**581** - Link interface incident - implicit incident.

**582** - Link interface incident - bit-error threshold exceeded.

**583** - Link failure - loss of signal or loss of synchronization.

**584** - Link failure - not-operational primitive sequence (NOS) received.

**585** - Link failure - primitive sequence timeout.

**586** - Link failure - invalid primitive sequence received for the current link state.

Were one or more event codes found?

**YES    NO**



Perform director fault isolation at the management server or customer-supplied server running the EFCM Lite application.

**Go to [step 3](#).**

Go to [Table 3-3](#) on page 3-3 to interpret event codes.

## MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the director power distribution system, including defective AC power cords, redundant power supplies, or the AC module.

### 1

Was an event code **200**, **201**, **202**, or **208** observed at the *Intrepid 6140 Event Log* (management server) or at the SANpilot event log?

**YES    NO**



**Go to [step 10](#).**

## 2

Table 3-4 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

**Table 3-4 MAP 100: Event Codes**

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to <a href="#">step 3</a> .
201	Power supply DC voltage failure.	Go to <a href="#">step 3</a> .
202	Power supply thermal failure.	Go to <a href="#">step 7</a> .
208	Power supply false shutdown.	Go to <a href="#">step 8</a> .

## 3

A redundant power supply is disconnected from facility power, not properly installed, or has failed.

Verify the power supply is connected to facility power.

- Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the director and a facility power receptacle. If not, connect the cord as directed by the customer.
- Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.
- Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

**YES    NO**



**Go to [step 5](#).**

## 4

Verify redundant power supply operation.

- Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
- At the management server *Hardware View*, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

**YES NO**

↓ The director appears operational. **Exit MAP.**

## 5

Ensure the power supply is correctly installed and seated in the director. If required, partially remove and reseal the power supply.

Was a corrective action performed?

**YES NO**

↓ **Go to [step 7](#).**

## 6

Verify redundant power supply operation.

- a. Inspect the power supply and ensure the green **PWR OK** LED illuminates and all amber LEDs extinguish.
- b. At the management server *Hardware View*, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

**YES NO**

↓ The director appears operational. **Exit MAP.**

## 7

A redundant power supply failed and must be removed and replaced ([RRP: Power Supply](#) on page 5-20).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove a power supply unless a replacement is immediately available. To avoid director overheating, a power supply must be replaced within five minutes.

---

Did power supply replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 8

Power sense circuitry is defective in the indicated power supply or there is a problem with facility input power.

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 180 and 264 VAC, and at least 15 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

**NO YES**

↓ **Go to [step 7](#).**

Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

## 9

Verify director operation:

- a. Inspect the director front bezel and ensure the green power LED illuminates. Inspect the active CTP card and ensure the green LED illuminates.
- b. Inspect both power supplies. Ensure both green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
- c. At the management server *Hardware View*, observe all graphics representing FRUs and power supplies, and ensure emulated green LEDs illuminate.

Is a failure indicated?

**YES NO**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 10

Is fault isolation being performed at the director?

**YES NO**



Fault isolation is being performed at the management server, customer-supplied server, or SANpilot interface. **Go to step 21.**

## 11

Verify the director is connected to facility power and is powered on.

- a. Ensure AC power cords (**PS0** and **PS1**) are connected to the rear of the director and to facility power receptacles. If not, connect the cords as directed by the customer.
- b. Ensure associated facility circuit breakers are on. If not, ask the customer set the circuit breakers on.
- c. Ensure the AC power cords are not damaged. If damaged, replace the cords.

**Continue.**

## 12

Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**



**Go to step 14.**

## 13

Does inspection of a power supply indicate a failure (green **PWR OK** LED extinguished and one or more amber LEDs illuminated)?

**NO YES**



A redundant power supply failed. **Go to step 7.**

The director appears operational. **Exit MAP.**

## 14

The director AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- AC module.
- Backplane.

Does inspection of both power supplies indicate a dual failure (both green **PWR OK** LEDs extinguished and one or more amber LEDs illuminated on each power supply)?

**YES NO**

- ↓ One or both power supplies appear operational, but a power distribution failure through the backplane is indicated.  
**Go to step 19.**

## 15

Ensure both power supplies are correctly installed and seated in the director. If required, partially remove and reseal the power supplies.

Was a corrective action performed?

**YES NO**

- ↓ **Go to step 17.**

## 16

Verify operation of both power supplies.

- a. Inspect the power supplies and ensure the green **PWR OK** LEDs illuminate and all amber LEDs extinguish.
- b. At the management server *Hardware View*, observe the graphics representing the power supplies and ensure failure symbols (blinking red and yellow diamonds) do not appear.

Is a dual power supply failure still indicated?

**YES NO**

- ↓ The director appears operational. **Exit MAP.**

## 17

Both power supplies failed and must be removed and replaced. (*RRP: Power Supply* on page 5-20). Perform the data collection procedure as part of FRU removal and replacement.

**ATTENTION!** Do not remove a power supply unless a replacement is immediately available. To avoid director overheating, a power supply must be replaced within five minutes.

Did dual power supply replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

A dual power supply failure is not confirmed. Replace both original power supplies. **Continue.**

## 18

An AC module failure is indicated and the FRU must be removed and replaced (*RRP: AC Module* on page 5-24). This procedure is nonconcurrent and must be performed while director power is off.

Did AC module replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

An AC module failure is not confirmed. Replace the original AC module. **Continue.**

## 19

One or both power supplies appear operational, but logic cards are not receiving DC power. In-card circuit breakers for all logic cards may have tripped due to a power surge, or the backplane failed.

Power cycle the director to reset all logic cards (*Power-On Procedure* on page 4-51).

Did power cycling the director solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

## 20

The backplane failed and must be removed and replaced (*RRP: Backplane* on page 5-35).

- This procedure is nonconcurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 21

Is fault isolation being performed at the management server or customer-supplied server?

**YES      NO**

↓      Fault isolation is being performed at the SANpilot interface.  
**Go to [step 25](#).**

## 22

At the *Hardware View*, does a yellow triangle appear at the alert panel and a blinking red and yellow diamond (failed FRU indicator) appear to overlay a power supply graphic?

**NO      YES**

↓      A redundant power supply failed. **Go to [step 7](#).**

## 23

At the *Hardware View*, does a grey square appear at the alert panel, a **No Link** status appear at the *Intrepid 6140 Status* table, and graphical FRUs appear uninstalled?

**YES      NO**

↓      A green circle appears at the alert panel and the director appears operational. **Exit MAP.**

The grey square indicates the management server or customer-supplied server cannot communicate with the director because:

- The director-to-server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 24

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:



- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES    NO**

↓    **Go to [step 14](#).**

Analysis for an Ethernet link or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-9. If this is the second time at this step, contact the next level of support. **Exit MAP.**

## 25

Does the SANpilot interface appear operational?

**NO    YES**

↓    **Go to [step 28](#).**

## 26

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 27

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**

↓ **Go to step 14.**

Analysis for an Ethernet link or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-9. If this is the second time at this step, contact the next level of support. **Exit MAP.**

## 28

Inspect power supply operational states at the SANpilot interface.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- b. Inspect the *Status* fields for both power supplies.

Does the *Status* field display a **Failed** message for either power supply?

**NO YES**

↓ A redundant power supply failed. **Go to step 7.**

The director appears operational. **Exit MAP.**

## MAP 0200: POST Failure Analysis

When the director is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the director performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL.

If an error is detected, the POST/IPL continues in an attempt to initialize the director and bring it online. An event code **400** displays when the director completes the POST/IPL.

### 1

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.

- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**

- ↓ An AC power distribution problem is indicated, and analysis for the failure is not described in this MAP. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 2

Was an event code **400**, **411**, or **413** observed at the *Intrepid 6140 Event Log* or at the SANpilot event log?

**YES NO**

- ↓ Analysis for the failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-9. **Exit MAP.**

## 3

[Table 3-5](#) lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

**Table 3-5 MAP 200: Event Codes**

Event Code	Explanation	Action
<b>400</b>	Power-up diagnostic failure.	Go to <a href="#">step 4</a> .
<b>411</b>	Firmware fault.	Go to <a href="#">step 11</a> .
<b>413</b>	Backup CTP card POST failure.	Go to <a href="#">step 12</a> .

## 4

POST/IPL diagnostics detected a FRU failure.

- At the *Intrepid 6140 Event Log* or the SANpilot event log, examine the first two bytes (**0** and **1**) of event data associated with event code **400**.
- Byte **0** is a FRU code that indicates the failed component. Byte **1** is the slot number of the failed FRU (**00** for a nonredundant FRU, **00** or **01** for redundant FRUs, and **00** through **34** for port cards).

Table 3-6 lists byte 0 FRU codes and associated steps that describe fault isolation procedures.

**Table 3-6 MAP 200: Byte 0 FRU Codes**

Byte 0	Failed FRU	Action
01	Backplane.	Go to <a href="#">step 5</a> .
02	CTP card.	Go to <a href="#">step 6</a> .
03	SBAR assembly.	Go to <a href="#">step 7</a> .
05	Fan module.	Go to <a href="#">step 8</a> .
06	Power supply.	Go to <a href="#">step 9</a> .
08 - 0F	Port card.	Go to <a href="#">step 10</a> .

## 5

The backplane failed POSTs (indicated by a FRU code **01**) and must be removed and replaced (*RRP: Backplane* on page 5-35).

- This procedure is nonconcurrent and must be performed while director power is off.
- Perform the data collection procedure as part of FRU removal and replacement.

Did backplane replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 6

A CTP card failed POSTs (indicated by a FRU code **02**) and must be removed and replaced (*RRP: CTP Card* on page 5-6).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove and replace a redundant CTP card if the backup CTP card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP card replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 7

An SBAR assembly failed POSTs (indicated by a FRU code **03**) and must be removed and replaced (*RRP: SBAR Assembly* on page 5-31).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 8

A fan module failed POSTs (indicated by a FRU code **05**) and must be removed and replaced (*RRP: Fan Module* on page 5-27).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

---

Did fan module replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 9

A power supply failed POSTs (indicated by a FRU code **06**) and must be removed and replaced (*RRP: Power Supply* on page 5-20).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove a power supply unless a replacement is immediately available. To avoid director overheating, a power supply must be replaced within five minutes.

---

Did power supply replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 10

A port card failed POSTs (indicated by FRU codes **08** through **0F**) and must be removed and replaced (*RRP: Port Module Card (UPM and XPM)* on page 5-10).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did port card replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

**11**

POST/IPL diagnostics detected a firmware failure and performed an online dump. All Fibre Channel ports reset after the failure and devices momentarily logout, login, and resume operation.

Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

**12**

The backup CTP card failed POST/IPL diagnostics, and must be removed and replaced (*RRP: CTP Card* on page 5-6).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove and replace a redundant CTP card if the backup CTP card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP card replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## MAP 0300: Server Application Problem Determination

This map describes isolation of management server or customer-supplied server application problems, including problems associated with the Windows 2000 Professional operating system, SAN management application (EFCM or SANavigator), or Intrepid 6140 Element Manager application.

**1**

Did the management server or customer-supplied server lock up or crash without displaying a warning or error message?

**YES      NO**

↓      Go to **step 4.**

## 2

An application or operating system problem is indicated. Close the SAN management application (at the browser-capable PC connected through an Ethernet LAN segment to the management server).

- a. At the management server Windows 2000 desktop, click the **Send Ctrl-Alt-Del** button at the top of the window. The *Windows Security* dialog box displays ([Figure 3-13](#)).

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action controls the browser-capable PC, not the rack-mount management server.

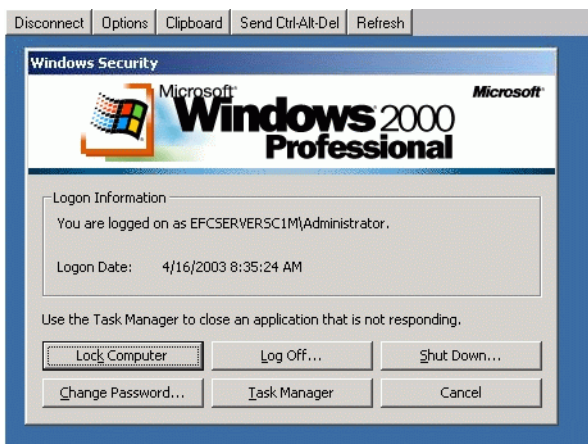
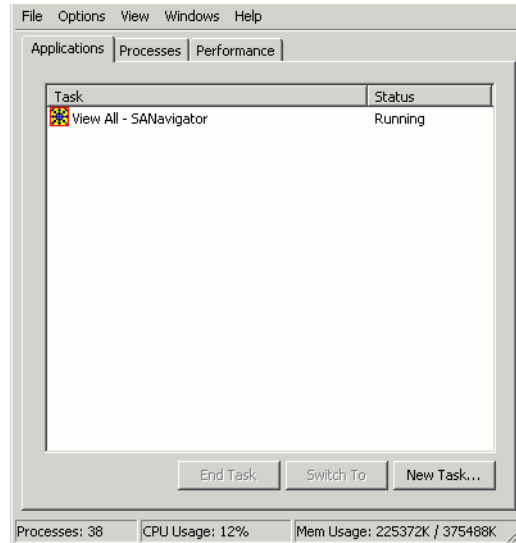


Figure 3-13 Windows Security Dialog Box

- b. Click *Task Manager*. The *Windows Task Manager* dialog box displays with the *Applications* page open ([Figure 3-14](#)).





**Figure 3-14 Windows Task Manager Dialog Box (Applications Page)**

- c. Select (highlight) the *EFCM* or *SANavigator* entry and click *End Task*. The SAN management application closes.

**Continue.**

### 3

Attempt to clear the problem by rebooting the management server or customer-supplied server PC. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-15).



**Figure 3-15 Shut Down Windows Dialog Box**

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power ( $\Phi$ ) button on the LCD panel to power on the server and perform POSTs. During POSTs:
  1. The green LCD panel illuminates.
  2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-16):

**Boot from LAN?**  
**Press <Enter>**

**Figure 3-16 LCD Panel During Boot Sequence**

4. Ignore the message. After ten seconds, the server performs the boot sequence from the BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.

- CPU temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
  - e. After rebooting the server at the LCD panel, log on to the management server Windows 2000 desktop through a LAN connection to a browser-capable PC ([Access the Management Server Desktop](#) on page 2-26). The SAN management application starts and the *EFCM Log In* or *SANavigator Log In* dialog box displays ([Figure 3-3](#)).
  - f. Type a user name and password, and click *Login*. The SAN management application opens and the EFCM or SANavigator main window displays ([Figure 3-4](#)).

Did the main window display and does the SAN management appear operational?

**NO      YES**

↓      The problem is transient and the management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 4

Did the SAN management application display a dialog box with the message **Connection to management server lost - click OK to exit application** or **EFCM or SANavigator error *n*** (where *n* is an error message number 1 through 8 inclusive)?

**NO      YES**

↓      A SAN management application error occurred. Click *OK* to close the window and close the application. **Go to [step 3](#).**

## 5

Did the SAN management application display a window with the message **The software version on this management server is not compatible with the version on the remote management server?**

**YES      NO**

↓      **Go to [step 8](#).**

## 6

The SAN management applications running on the management server and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want the SAN management application upgraded?

**YES    NO**

↓      Power off the client workstation. **Exit MAP.**

## 7

Upgrade the downlevel SAN management application ([Installing or Upgrading Software](#) on page 4-82).

Did the software upgrade solve the problem?

**NO    YES**

↓      The management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 8

Did the Element Manager application display a window with the message **Element Manager error 5001** or **Element Manager error 5002**?

**NO    YES**

↓      A Element Manager application error occurred. Click *OK* to close the window and close the SAN management and Element Manager applications. **Go to [step 3](#).**

## 9

Did the Element Manager application display a window with the message **Send firmware failed**?

**YES    NO**

↓      **Go to [step 11](#).**

## 10

An attempt to download a firmware version from the management server or customer-supplied server hard drive to the director failed. Retry the operation ([Managing Firmware Versions](#) on page 4-55).

Did the firmware version download to the director?

**NO      YES**



The management server or customer-supplied server appears operational. **Exit MAP.**

A CTP card failure is suspected. Go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem. **Exit MAP.**

## 11

Did the Element Manager application display a window with the message **The data collection process failed**?

**YES      NO**



**Go to [step 13](#).**

## 12

The data collection failed. Retry the process using a new CD ([Collecting Maintenance Data](#) on page 4-39).

Did the data collection complete?

**NO      YES**



**Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 13

Did the management server or customer-supplied server lock up or crash and display a *Dr. Watson for Windows 2000* dialog box ([Figure 3-17](#))?

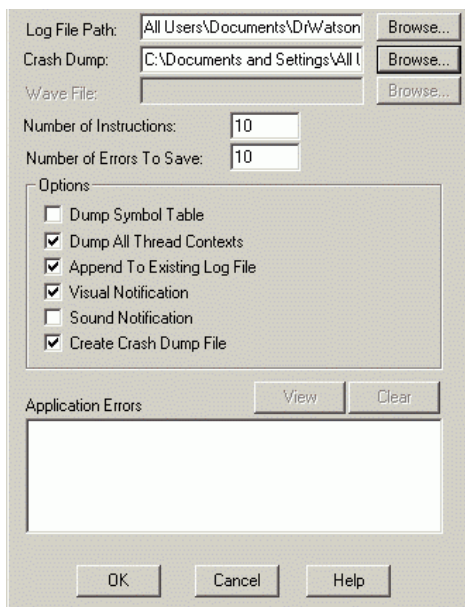


Figure 3-17 Dr. Watson for Windows 2000 Dialog Box

YES NO



Go to [step 14](#).

A SAN management application error occurred and transmitted a handling exception event to the operating system.

- a. Click *Cancel* to close the *Dr. Watson for Windows 2000* dialog box and SAN management application.
- b. Using the *My Computer* function at the Windows 2000 desktop, copy the crash dump file (**user.dmp**) from the local disk (**C:**) to the CD-RW drive (**D:**).
- c. At the management server, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
- d. Remove the CD and return it to McDATA customer support personnel for analysis.

Go to [step 3](#).

## 14

Did the management server or customer-supplied server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

**YES    NO**



The management server or customer-supplied server appears operational. **Exit MAP.**

## 15

Attempt to clear the problem by power cycling the management server or customer-supplied server PC. If the customer-supplied server does not use the Windows 2000 operating system, refer to the supporting documentation to reboot the server.

- a. At the rack-mount management server, press the power (⏻) button on the LCD panel to power off the server.
- b. Wait approximately 30 seconds and press the power (⏻) button to power on the server and perform POSTs. During POSTs:
  1. The green LCD panel illuminates.
  2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-18):



**Boot from LAN?**  
**Press <Enter>**

**Figure 3-18    LCD Panel During Boot Sequence**

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.

- Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - CPU temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
- c. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
  - d. After rebooting the server at the LCD panel, log on to the management server Windows 2000 desktop through a LAN connection to a browser-capable PC ([Access the Management Server Desktop](#) on page 2-26). The SAN management application starts and the *EFCM Log In* or *SANavigator Log In* dialog box displays ([Figure 3-3](#)).
  - e. Type a user name and password, and click *Login*. The SAN management application opens and the EFCM or SANavigator or EFCM main window displays ([Figure 3-4](#)).

Did the main window display and does the SAN management application appear operational?

**NO      YES**

↓      The problem is transient and the management server or customer-supplied server appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## MAP 0400: Loss of Server Communication

This MAP describes fault isolation of the Ethernet communication link between a director and the management server or customer-supplied server, or between a director and a web browser PC running the SANpilot interface. Failure indicators include:

- Event codes recorded at the *Intrepid 6140 Event Log* or SANpilot event log.
- At the EFCM or SANavigator main window, a grey square with an exclamation mark associated with the icon representing the director reporting the problem.
- At the *Hardware View*, a grey square at the alert panel, a **No Link** status and reason at the *Intrepid 6140 Status* table, and no FRUs visible for the director.



- At the web browser PC, A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or similar message.

It may take up to five minutes for the link to activate at the EFCM or SANavigator main window after the logical connection between the director and management server or customer-supplied server is initiated. This delay is normal.

**ATTENTION!** Prior to servicing a director, management server, or customer-supplied server, determine the Ethernet LAN configuration. Installation of directors and the server on a public customer intranet can complicate problem determination and fault isolation.

## 1

Was an event code **430**, **431**, or **432** observed at the *Intrepid 6140 Event Log* or at the SANpilot event log?

**YES NO**



Go to **step 3**.

## 2

**Table 3-7** lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 3-7 MAP 400: Event Codes**

Event Code	Explanation	Action
430	Excessive Ethernet transmit errors.	Go to <b>step 8</b> .
431	Excessive Ethernet receive errors.	Go to <b>step 8</b> .
432	Ethernet adapter reset.	Go to <b>step 14</b> .

## 3

Is fault isolation being performed at the management server or customer-supplied server?

**YES NO**



Fault isolation is being performed through the SANpilot interface. Go to **step 24**.

## 4

At the EFCM or SANavigator main window, is a grey square with yellow exclamation mark associated with the icon representing the director reporting the problem?

**YES    NO**

↓    The director-to-server connection is restored and appears operational. **Exit MAP.**

The status symbol indicates the management server or customer-supplied server cannot communicate with the director because:

- The director-to-server Ethernet link failed.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 5

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES    NO**

↓    A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 6

At the director, inspect the amber LED at the top of each CTP card. Is the amber LED illuminated on both CTP cards?

**NO    YES**

↓    Failure of both CTP cards is indicated. Go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 7

The director-to-server Ethernet link failed. At the physical map, right-click the icon with the grey square and exclamation mark representing the director or switch reporting the problem. A pop-up menu appears. Select the *Element Manager* option from the menu. The Element Manager application opens and the *Hardware View* displays. At the *Hardware View*:

- A grey square appears at the alert panel.
- No FRUs are visible for the director.
- The *Intrepid 6140 Status* table is yellow, the *Status* field displays **No Link**, and the **Reason** field displays an error message.

Table 3-8 lists the error messages and associated steps that describe fault isolation procedures.

**Table 3-8 MAP 400: Error Messages**

Error Message	Action
Never connected.	Go to <a href="#">step 8</a> .
Link timeout.	Go to <a href="#">step 8</a> .
Protocol mismatch.	Go to <a href="#">step 15</a> .
Duplicate session.	Go to <a href="#">step 18</a> .
Unknown network address.	Go to <a href="#">step 21</a> .
Incorrect product type.	Go to <a href="#">step 23</a> .

## 8

Transmit or receive errors for a director Ethernet adapter (on each CTP card) exceeded a threshold, the director-to-server link was not connected, or the director-to-server link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the director is connected to the management server or customer-supplied server through one or more Ethernet hubs.

- Ensure an RJ-45 Ethernet cable connects both of the director CTP cards to an Ethernet hub. If not, connect the cables as directed by the customer.

- b. Ensure an RJ-45 Ethernet cable connects the management server to an Ethernet hub. If not, connect the cable as directed by the customer.
- c. Ensure the Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

**NO**      **YES**



**Go to [step 1](#).**

**9**

Does the LAN configuration use multiple (up to four) Ethernet hubs that are daisy-chained?

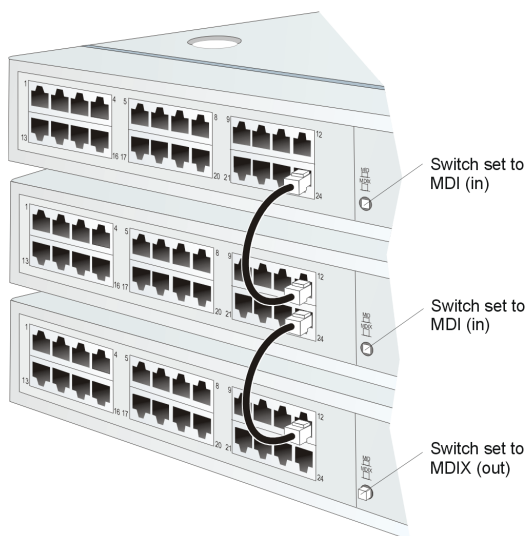
**YES**      **NO**



**Go to [step 11](#).**

**10**

Verify the hubs are correctly daisy-chained ([Figure 3-19](#).)



**Figure 3-19 Ethernet Hubs, Daisy-Chained**

**NOTE:** To check two hubs, use [step a](#) and [step b](#) (top and middle hub instructions only).

- a. At the first (top) Ethernet hub, ensure an RJ-45 Ethernet patch cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI** (in).
- b. At the middle Ethernet hub, ensure the patch cable from the top hub connects to port **12**, the patch cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI** (in).
- c. At the bottom Ethernet hub, ensure the patch cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX** (out).

Was a corrective action performed?

**NO**      **YES**

↓      **Go to [step 1](#).**

## 11

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a hub failure indicated?

**YES**      **NO**

↓      **Go to [step 13](#).**

## 12

Remove and replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

**NO**      **YES**

↓      The director-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 13

A problem with another LAN-attached device is indicated.

- If the problem is associated with another director or management server or customer-supplied server, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem for that device. **Exit MAP.**

- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

**NO      YES**

↓      The director-to-server connection is restored and appears operational. **Exit MAP.**

## 14

The Ethernet adapter on the director active CTP card reset in response to an error. The connection to the management server or customer-supplied server terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

## 15

A protocol mismatch occurred because the SAN management application and the director firmware are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does the SAN management application require upgrade?

**YES      NO**

↓      **Go to [step 17](#).**

## 16

Upgrade the SAN management application ([Installing or Upgrading Software](#) on page 4-82).

Did the director-to-server Ethernet connection recover?

**NO      YES**

↓      The director-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 17

A director firmware upgrade is required ([Download a Firmware Version to a Director](#) on page 4-63). Perform the data collection procedure after the download.

Did the director-to-server Ethernet connection recover?

**NO YES**

↓ The director-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 18

An instance of the SAN management application is open at another management server or customer-supplied server and communicating with the director (duplicate session). Notify the customer and:

- Power off the management server or customer-supplied server running the second instance of the application, or
- Configure the management server or customer-supplied server running the second instance of the application as a client workstation.

Does the customer want the second management server or customer-supplied server configured as a client?

**YES NO**

↓ Power off the management server or customer-supplied server reporting the **Duplicate Session** communication problem. **Exit MAP.**

## 19

Determine the internet protocol (IP) address of the management server or customer-supplied server running the first instance of the SAN management application.

- a. After the management server powers on and successfully completes POSTs, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays the following operational information:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - CPU temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.

- b. After a few seconds, the LCD panel displays the following (Figure 3-20):



LAN 2:  
010.001.001.001

Figure 3-20 LCD Panel (LAN 2 IP Address)

- c. Depending on switch-to-server LAN connectivity, record the appropriate IP address (LAN 1 or LAN 2).

**Continue.**

## 20

Configure the management server or customer-supplied server reporting the **Duplicate Session** communication problem as a client.

- a. At the EFCM or SANavigator main window, select *Logout* from the *SAN* menu. The application logs out and the *EFCM Log In* or *SANavigator Log In* dialog box displays (Figure 3-3).
- b. Type a user name and password.
- c. Type the IP address of the management server or customer-supplied server running the first instance of the SAN management application in the *Network Address* field.
- d. Click *Login*. The SAN management application opens and the EFCM or SANavigator main window displays (Figure 3-4).

Did the management server or customer-supplied server reconfigure as a client and did the Ethernet connection recover?

**NO      YES**



The director-to-server connection is restored and the second management server or customer-supplied server appears operational as a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 21

The IP address defining the director to the SAN management application is incorrect or unknown and must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the director IP address. The tools are

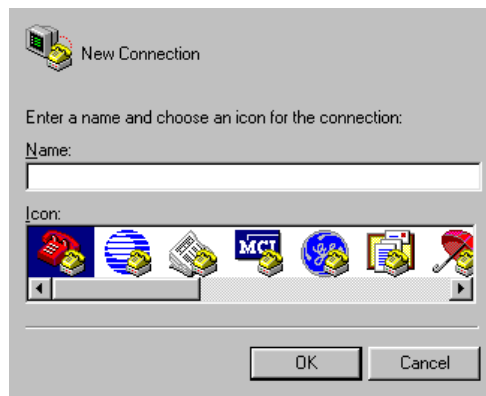


provided with the director or by service personnel. To verify the IP address:

- a. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a phillips-tip screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.
- b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
- c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
- d. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

**NOTE:** The following steps describe inspecting the IP address using HyperTerminal serial communication software.

- e. At the *Windows Workstation* menu, sequentially select *Programs*, *Accessories*, *Hyperterminal*, and *HyperTerminal*. The *Connection Description* dialog box displays (Figure 3-21).



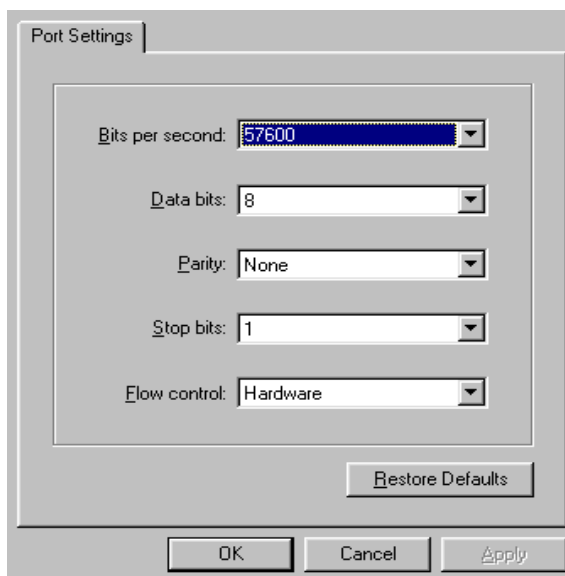
**Figure 3-21** Connection Description Dialog Box

- f. Type **Intrepid 6140** in the *Name* field and click *OK*. The *Connect To* dialog box displays (Figure 3-22).



**Figure 3-22 Connect To Dialog Box**

- g. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the serial communication port connection to the director), and click **OK**. The *COMn* dialog box (Figure 3-23) displays (where *n* is 1 or 2).



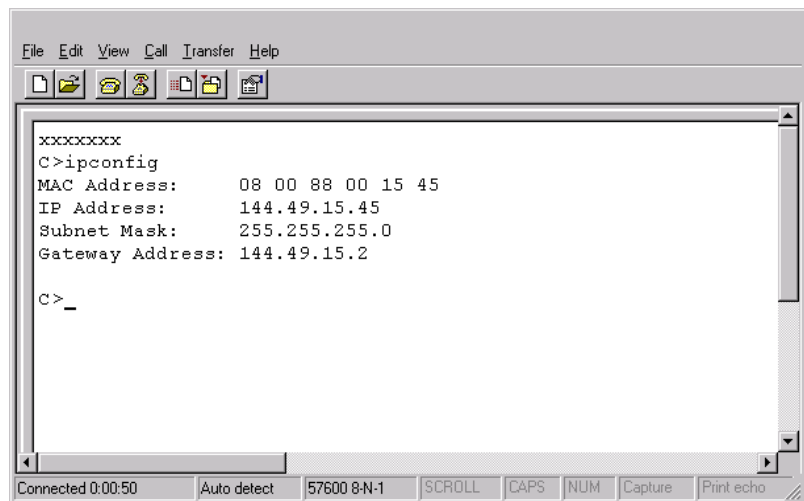
**Figure 3-23 COMn Properties Dialog Box**

- h. Configure the *Port Settings* parameters as follows:
  - Bits per second - **115200**.

- Data bits - **8**.
- Parity - **None**.
- Stop bits - **1**.
- Flow control - **Hardware** or **None**.

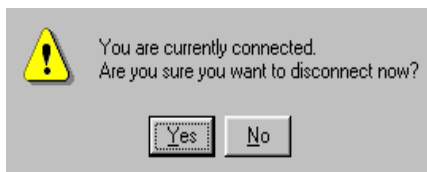
When the parameters are set, click **OK**. The *Intrepid 6140 - HyperTerminal* dialog box displays.

- i. At the **>** prompt, type the user-level password (the default is **password**) and press **Enter**. The password is case sensitive. The *Intrepid 6140 - HyperTerminal* dialog box displays with a **C>** prompt at the bottom of the window.
- j. At the **C>** prompt, type **ipconfig** and press **Enter**. The *Intrepid 6140 - HyperTerminal* dialog box (Figure 3-24) displays with configuration information listed, including the IP address.



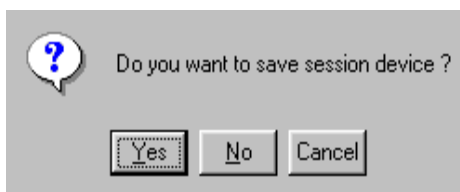
**Figure 3-24** Intrepid 6140 - HyperTerminal Dialog Box

- k. Record the director IP address.
- l. Select *Exit* from the *File* pull-down menu to close the HyperTerminal application. A *HyperTerminal* dialog box displays (Figure 3-25).



**Figure 3-25 HyperTerminal Dialog Box**

- m. Click Yes. A second *HyperTerminal* dialog box displays (Figure 3-26).



**Figure 3-26 HyperTerminal Dialog Box**

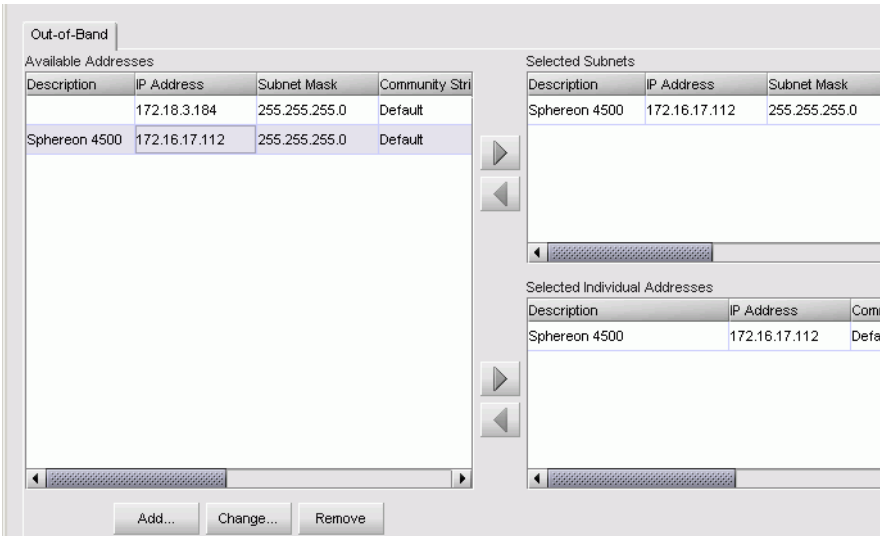
- n. Click *No* to exit and close the HyperTerminal application.
- o. Power off the maintenance terminal.
- p. Disconnect the RS-232 null modem cable from the director and the maintenance terminal. Replace the protective cap over the maintenance port.

**Continue.**

## 22

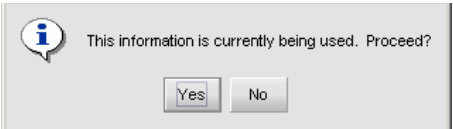
Define the director IP address to the management server or customer-supplied server.

- a. At the SAN management application (EFCM or SANavigator main window), select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 3-27).



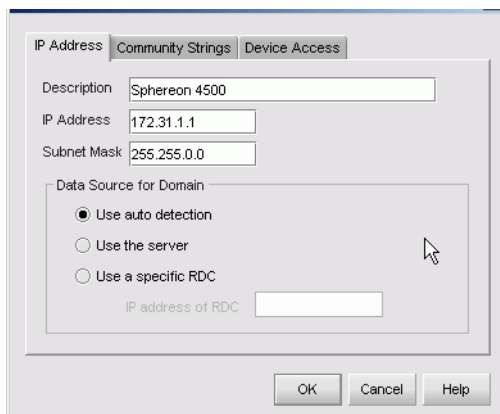
**Figure 3-27 Discover Setup Dialog Box**

- b. At the *Available Addresses* field, select (highlight) the director to be reconfigured and click *Change*. The *Editing Domain Information* dialog box displays (Figure 3-28).



**Figure 3-28 Editing Domain Information Dialog Box**

- c. Click *Yes*. The *Domain Information* dialog box displays with the *IP Address* page open (Figure 3-29).



**Figure 3-29 Domain Information Dialog Box (IP Address Page)**

- d. Type the correct IP address in the *IP Address* field.
- e. Click *OK* to save the new IP address, close the dialog box, and redefine the director to the SAN management application.
- f. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.

At the SAN management application master log, did the director IP address change to the new entry and did the Ethernet connection recover?

**NO YES**



The director-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 23

An incorrect product type is defined to the management server or customer-supplied server.

- a. Right-click the product icon with a grey square and yellow exclamation mark (representing the director reporting the problem) at the SAN management application physical map. A pop-up menu appears.
- b. Select the *Delete* option from the pop-up menu. The *EFCM* or *SANavigator Message* dialog box displays (Figure 3-30).



**Figure 3-30 EFCM or SANavigator Message Dialog Box**

- c. Click **Yes** to delete the director.
- d. At the SAN management application main window, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 3-27).
- e. Click *Add*. The *Domain Information* dialog box displays with the *IP Address* page open (Figure 3-31).



**Figure 3-31 Domain Information Dialog Box (IP Address Page)**

- f. Type a director description in the *Description* field.
- g. Type the IP address (determined by the customer network administrator) in the *IP Address* field.
- h. Type the subnet mask (determined by the customer network administrator) in the *Subnet Mask* field.
- i. At the *Data Source for Domain* area of the dialog box, select the *Use auto detection*, *Use the server*, or *Use a specific RDC* button (determined by the customer network administrator).

- j. Click *OK* to save the information, close the dialog box, and define the new configuration to the SAN management application.
- k. Click *OK* to close the *Discover Setup* dialog box and return to the SAN management application.

At the SAN management application master log, did the director IP address change to the new configuration and did the Ethernet connection recover?

**NO      YES**

- ↓      The director-to-server connection is restored and appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 24

Does the SANpilot interface appear operational?

**NO      YES**

- ↓      The director-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

## 25

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the director because:

- The director-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 26

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card, and illuminated green **PWR OK** LEDs on both power supplies.



- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**

- ↓ A power distribution problem is indicated. Go to [MAP 0100: Power Distribution Analysis](#) on page 3-33. **Exit MAP.**

## 27

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

**NO YES**

- ↓ Failure of both CTP cards is indicated. Go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## 28

Either a director-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a director Ethernet port failure is indicated.

- a. Wait approximately five minutes, then attempt to login to the director again.
- b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the director. The *Username and Password Required* dialog box appears.
- c. Type the user name and password, and click *OK*. If the *View* panel does not display, wait five minutes and perform this step again.

Does the SANpilot interface appear operational with the *View* panel displayed?

**NO YES**

- ↓ The director-to-SANpilot PC connection is restored and appears operational. **Exit MAP.**

Failure of the CTP card Ethernet port is indicated. Go to [MAP 0500: FRU Failure Analysis](#) on page 3-74. **Exit MAP.**

## MAP 0500: FRU Failure Analysis

This MAP describes fault isolation for the CTP card, SBAR assembly, and fan module. Failure indicators include:

- An event code recorded at the *Intrepid 6140 Event Log* (management server) or the SANpilot event log.
- The amber LED on the FRU illuminates.
- An amber emulated LED on a FRU graphic at the *Hardware View* illuminates.
- A blinking red and yellow diamond (failed FRU indicator) appears over a FRU graphic; or a grey square (status unknown indicator) or yellow triangle (attention indicator) appears at the alert panel of the *Hardware View*.
- A **Failed** message associated with a FRU at the SANpilot interface.

### 1

Was an event code **300, 301, 302, 303, 304, 305, 414, 420, 426, 433, 440, 604, 605, 607, 620, 805, 806, 807, 810, 811, 812, or 850** observed at the *Intrepid 6140 Event Log* or at the SANpilot event log?

YES    NO



Go to [step 3](#).

### 2

[Table 3-9](#) lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 3-9    MAP 500: Event Codes**

Event Code	Explanation	Action
300	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .
301	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .
302	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .
303	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .
304	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .
305	Cooling fan propeller failed.	Go to <a href="#">step 5</a> .

Table 3-9 MAP 500: Event Codes (*continued*)

Event Code	Explanation	Action
414	Backup CTP card failed.	Go to <a href="#">step 7</a> .
420	Backup CTP card NV-RAM failure.	Go to <a href="#">step 7</a> .
426	Multiple ECC single-bit errors occurred.	Go to <a href="#">step 7</a> .
433	Non-recoverable Ethernet fault.	Go to <a href="#">step 7</a> .
440	Embedded port hardware failed.	Go to <a href="#">step 7</a> .
604	SBAR assembly failure.	Go to <a href="#">step 9</a> .
605	SBAR assembly revision not supported.	Go to <a href="#">step 16</a> .
607	Director contains no operational SBAR assemblies.	Go to <a href="#">step 9</a> .
620	SBAR fan failure.	Go to <a href="#">step 5</a> .
805	High temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">step 9</a> .
806	Critically hot temperature warning (SBAR assembly thermal sensor).	Go to <a href="#">step 9</a> .
807	SBAR assembly shutdown due to thermal violation.	Go to <a href="#">step 9</a> .
810	High temperature warning (CTP card thermal sensor).	Go to <a href="#">step 7</a> .
811	Critically hot temperature warning (CTP card thermal sensor).	Go to <a href="#">step 7</a> .
812	CTP card shutdown due to thermal violation.	Go to <a href="#">step 7</a> .
850	System shutdown due to CTP card thermal violations.	Go to <a href="#">step 7</a> .

### 3

Is fault isolation being performed at the director?

**YES NO**



Fault isolation is being performed at the management server or customer-supplied server, or SANpilot interface. **Go to [step 10](#).**

## 4

Inspect both fan modules at the rear of the director. Fan module LEDs can be inspected through the hexagonal cooling vents of the radio frequency interference (RFI) shield.

Does inspection of a director fan module indicate a failure? Indicators include:

- The amber LED is illuminated but not blinking (beaconing) on one or both fan modules.
- One or more cooling fans are not rotating.

**YES    NO**



**Go to [step 6](#).**

## 5

One or more cooling fans failed. One or both fan modules ([RRP: Fan Module](#) on page 5-27), or one or both SBAR assemblies ([RRP: SBAR Assembly](#) on page 5-31) must be removed and replaced.

- If a multiple fan failure caused a thermal shutdown, power on the director after the fan modules are replaced ([Power-On Procedure](#) on page 4-51).

---

**ATTENTION!** Do not remove a fan module unless the replacement module is available. Operation of the director with only one fan module for an extended period may cause one or more thermal sensors to post event codes.

---

Do the fan modules appear to function?

**NO    YES**



The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 6

Inspect the faceplates of both CTP cards at the front of the director.

Is the amber LED at the top of a CTP card illuminated but not blinking (beaconing)?

**YES    NO**



**Go to [step 8](#).**

## 7

A CTP card failed and must be removed and replaced ([RRP: CTP Card](#) on page 5-6).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

---

**ATTENTION!** Do not remove and replace a CTP card if the backup CTP card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

---

Did CTP card replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 8

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

**YES      NO**

↓      The director appears operational. **Exit MAP.**

## 9

An SBAR assembly failed and must be removed and replaced ([RRP: SBAR Assembly](#) on page 5-31).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

**10**

Is fault isolation being performed at the management server or customer-supplied server?

**YES NO**



Fault isolation is being performed at the SANpilot interface.  
**Go to [step 18](#).**

**11**

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay a fan module graphic at the *Hardware View*?

**NO YES**



A fan module failure is indicated. **Go to [step 5](#).**

**12**

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay a CTP card graphic at the *Hardware View*?

**NO YES**



A CTP card failure is indicated. **Go to [step 7](#).**

**13**

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay an SBAR assembly graphic at the *Hardware View*?

**NO YES**



An SBAR assembly failure is indicated. **Go to [step 9](#).**

**14**

At the *Hardware View*, does a grey square appear at the alert panel, a **No Link** status appear at the *Intrepid 6140 Status* table, and graphical FRUs appear uninstalled?

**YES NO**



A green circle appears at the alert panel and the director appears operational. **Exit MAP.**

The grey square indicates the management server or customer-supplied server cannot communicate with the director because:

- The director-to-server Ethernet link failed.

- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 15

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

**NO      YES**



Failure of both CTP cards is indicated. **Go to step 7.**

Analysis for an Ethernet link or AC power distribution failure is not described in this MAP. Go to [MAP 0000: Start MAP](#) on page 3-9. If this is the second time at this step, contact the next level of support.

**Exit MAP.**

## 16

An SBAR assembly is not recognized by director firmware because the firmware version is not supported or the SBAR assembly failed. Advise the customer of the problem and determine the correct firmware version to download from the management server or customer-supplied server.

Download the firmware ([Download a Firmware Version to a Director](#) on page 4-63). Perform the data collection procedure after the download.

**Continue.**

## 17

Did the firmware download solve the problem?

**NO      YES**



The director appears operational. **Exit MAP.**

An SBAR assembly failure is indicated. **Go to step 9.**

## 18

Does the SANpilot interface appear operational?

**NO      YES**



**Go to step 22.**

## 19

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 20

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.
- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES    NO**



Analysis for an AC power distribution failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-9](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

## 21

At the director, inspect the amber LED at the top of each CTP card.

Is the amber LED illuminated on both CTP cards?

**NO    YES**



Failure of both CTP cards is indicated. **Go to step 7.**

Analysis for an Ethernet link failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-9](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**



## 22

Inspect fan module operational states at the SANpilot interface.

- a. At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- b. Inspect the *Status* fields for both fan modules.

Does the *Status* field display a **Failed** message for either fan module?

**NO**      **YES**

↓      A fan module failure is indicated. **Go to step 5.**

## 23

Inspect CTP card operational states at the SANpilot interface. Inspect the *Status* fields for both CTP cards.

Does the *Status* field display a **Failed** message for either CTP card?

**NO**      **YES**

↓      A CTP card failure is indicated. **Go to step 7.**

## 24

Inspect SBAR assembly operational states at the SANpilot interface. Inspect the *Status* fields for both assemblies.

Does the *Status* field display a **Failed** message for either SBAR assembly?

**NO**      **YES**

↓      An SBAR assembly failure is indicated. **Go to step 9.**

The director appears operational. **Exit MAP.**

## MAP 0600: Port Card Failure and Link Incident Analysis

This MAP describes fault isolation for UPM and XPM cards, SFP and XFP optical transceivers, and Fibre Channel link incidents. Failure indicators include:

- An event code recorded at the *Intrepid 6140 Event Log* or the SANpilot event log.
- One or more amber LEDs on the port card illuminate.
- One or more emulated amber LEDs on a port card graphic at the *Hardware View* illuminate.
- A blinking red and yellow diamond (failed FRU indicator) appears over a port card graphic or a yellow triangle (attention indicator) appears at the alert panel of the *Hardware View*.
- A port operational state message or a **Failed** message associated with a port card at the SANpilot interface.
- A link incident message recorded in the *Link Incident Log* or *Port Properties* dialog box.
- A link incident event code recorded at the console of an OSI or FICON server attached to the director reporting the problem.

**1**

Was an event code **080, 081, 504, 505, 506, 507, 512, 514, 800, 801,** or **802** observed at the *Intrepid 6140 Event Log* (management server) or at the SANpilot event log?

**NO      YES**

↓      **Go to step 3.**

**2**

Was an event code **581, 582, 583, 584, 585,** or **586** observed at the console of an OSI or FICON server attached to the director reporting the problem?

**YES      NO**

↓      **Go to step 4.**

## 3

Table 3-10 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 3-10 MAP 600: Event Codes**

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to <a href="#">step 18</a> .
081	Invalid attachment.	Go to <a href="#">step 19</a> .
504	Port card failure.	Go to <a href="#">step 6</a> .
505	Port card revision not supported.	Go to <a href="#">step 40</a> .
506	Fibre Channel port failure.	Go to <a href="#">step 6</a> .
507	Loopback diagnostics port failure.	Go to <a href="#">step 14</a> .
512	SFP/XFP optical transceiver nonfatal error.	Go to <a href="#">step 6</a> .
514	SFP/XFP optical transceiver failure.	Go to <a href="#">step 6</a> .
581	Implicit incident.	Go to <a href="#">step 33</a> .
582	Bit error threshold exceeded.	Go to <a href="#">step 33</a> .
583	Loss of signal or loss of synchronization.	Go to <a href="#">step 33</a> .
584	Not operational primitive sequence received.	Go to <a href="#">step 33</a> .
585	Primitive sequence timeout.	Go to <a href="#">step 33</a> .
586	Invalid primitive sequence received for current link state.	Go to <a href="#">step 33</a> .
800	High temperature warning (port card thermal sensor).	Go to <a href="#">step 7</a> .
801	Critically hot temperature warning (port card thermal sensor).	Go to <a href="#">step 7</a> .
802	Port card shutdown due to thermal violation.	Go to <a href="#">step 7</a> .

## 4

Is fault isolation being performed at the director?

**YES    NO**



Fault isolation is being performed at the management server, customer-supplied server, or SANpilot interface. **Go to step 8.**

## 5

Inspect the faceplates of port cards at the front of the director. Each card has an amber LED (at the top of the card) that illuminates if the card fails or if any Fibre Channel port fails.

Each card also has a bank of amber and green LEDs above the ports. Each LED pair is associated with a corresponding port (e.g. the top LED pair is associated with the top port). The amber LED illuminates and the green LED extinguishes if the port fails.

Are an amber port LED and the amber LED at the top of the port card illuminated but not blinking (beaconing)?

**YES    NO**



The director appears operational, however a link incident or other problem may have occurred. Perform fault isolation at the management server or customer-supplied server. **Go to step 8.**

## 6

A Fibre Channel port failed, and the SFP optical transceiver must be removed and replaced (*RRP: Optical Transceiver (SFP and XFP)* on page 5-15).

- This procedure is concurrent and can be performed while director power is on.
- Verify the location of the failed port. [Figure 3-32](#) and [Figure 3-33](#) show UPM card numbers (**0** through **34**), port numbers (**00** through **139**), and bolded logical port addresses.

UPM Cards								CTP - 1 Card	CTP - 0 Card	UPM Cards							
31	30	29	28	27	26	25	24			23	22	21	20	19	18	17	16
127	123	119	115	111	107	103	99			95	91	87	83	79	75	71	67
7F	7B	77	73	6F	6B	67	63			5F	5B	57	53	4F	4B	47	43
83	7F	7B	77	73	6F	6B	67			63	5F	5B	57	53	4F	4B	47
126	122	118	114	110	106	102	98			94	90	86	82	78	74	70	66
7E	7A	76	72	6E	6A	66	62			5E	5A	56	52	4E	4A	46	42
82	7E	7A	76	72	6E	6A	66			62	5E	5A	56	52	4E	4A	46
125	121	117	113	109	105	101	97			93	89	85	81	77	73	69	65
7D	79	75	71	6D	69	65	61			5D	59	55	51	4D	49	45	41
81	7D	79	75	71	6D	69	65	61	5D	59	55	51	4D	49	45		
124	120	116	112	108	104	100	96	92	88	84	80	76	72	68	64		
7C	78	74	70	6C	68	64	60	5C	58	54	50	4C	48	44	40		
80	7C	78	74	70	6C	68	64	60	5C	58	54	50	4C	48	44		
60	56	52	48	44	40	36	32	28	24	20	16	12	08	04	00		
3C	38	34	30	2C	28	24	20	1C	18	14	10	0C	08	04	00		
40	3C	38	34	30	2C	28	24	20	1C	18	14	10	0C	08	04		
61	57	53	49	45	41	37	33	29	25	21	17	13	09	05	01		
3D	39	35	31	2D	29	25	21	1D	19	15	11	0D	09	05	01		
41	3D	39	35	31	2D	29	25	21	1D	19	15	11	0D	09	05		
62	58	54	50	46	42	38	34	30	26	22	18	14	10	06	02		
3E	3A	36	32	2E	2A	26	22	1E	1A	16	12	0E	0A	06	02		
42	3E	3A	36	32	2E	2A	26	22	1E	1A	16	12	0E	0A	06		
63	59	55	51	47	43	39	35	31	27	23	19	15	11	07	03		
3F	3B	37	33	2F	2B	27	23	1F	1B	17	13	0F	0B	07	03		
43	3F	3B	37	33	2F	2B	27	23	1F	1B	17	13	0F	0B	07		
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		

Figure 3-32 UPM Card Diagram (Front)

UPM Cards			
34			
143 8F	142 8E	141 8D	140 8C
93	92	91	90

UPM Cards			
33			
136 88	137 89	138 8A	139 8B
8C	8D	8E	8F

32			
135 87	134 86	133 85	132 84
8B	8A	89	88

SBAR - 1 Module

SBAR - 0 Module

- This procedure is concurrent and can be performed while director power is on.
- Verify the location of the failed card. [Figure 3-32](#) and [Figure 3-33](#) show UPM card numbers (**0** through **34**), port numbers (**00** through **139**), and bolded logical port addresses.
- Notify the customer that all ports on the defective card are to be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
- Perform an external loopback test for all ports on the replacement card as part of FRU removal and replacement ([External Loopback Test \(Management Server\)](#) on page 4-32).
- Perform the data collection procedure as part of FRU removal and replacement ([Collecting Maintenance Data](#) on page 4-39).

Did port card replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 8

Is fault isolation being performed at the management server or customer-supplied server?

**YES NO**

↓ Fault isolation is being performed at the SANpilot interface.  
**Go to [step 42](#).**

## 9

Does a blinking red and yellow diamond (failed FRU indicator) appear to overlay a port card graphic at the *Hardware View*?

**NO YES**

↓ A port card failure is indicated. **Go to [step 6](#).**

## 10

Did a port card (all ports) fail a loopback test?

**NO YES**

↓ **Go to [step 14](#).**

## 11

Does a yellow triangle (attention indicator) appear to overlay a port card graphic at the *Hardware View*?

**YES NO**



**Go to [step 13](#).**

## 12

Inspect the port state and LED status for all ports with an attention indicator.

- a. At the *Hardware View*, double-click the port graphic with the attention indicator. The *Port Properties* dialog box displays.
- b. Inspect the *Operational State* field at the *Port Properties* dialog box, and the emulated green and amber LEDs adjacent to the port at the *Hardware View*.
- c. [Table 3-11](#) lists LED and port operational state combinations and associated MAP 0600 (or other) steps that describe fault isolation procedures.

**Table 3-11 Port Operational and LED States (Management Server)**

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to <a href="#">step 16</a> .
Not Operational	Off	Off	Go to <a href="#">step 16</a> .
Testing	Off	Blinking	Internal loopback test in process. <b>Exit MAP.</b>
Testing	On	Blinking	External loopback test in process. <b>Exit MAP.</b>
Beaconing	Off or On	Blinking	Go to <a href="#">step 17</a> .
Invalid Attachment	On	Off	Go to <a href="#">step 19</a> .
Link Reset	Off	Off	Go to <a href="#">step 32</a> .
Link Incident	Off	Off	Go to <a href="#">step 33</a> .
Segmented E_Port	On	Off	Go to <a href="#">MAP 0700</a> .

## 13

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the *Hardware View*, click *Logs* and select *Link Incident Log*. The *Link Incident Log* displays. If a link incident occurred, the affected port number is listed with one of the following messages.

**Link interface incident - implicit incident.**

**Link interface incident - bit-error threshold exceeded.**

**Link failure - loss of signal or loss of synchronization.**

**Link failure - not-operational primitive sequence (NOS) received.**

**Link failure - primitive sequence timeout.**

**Link failure - invalid primitive sequence received for the current link state.**

Did one of the listed messages appear in the *Link Incident Log*?

**YES    NO**

↓      The director appears operational. **Exit MAP.**

**Go to [step 33](#).**

## 14

A port card (all ports) failed an internal or external loopback test.

- a. Reset each port that failed the loopback test.
  1. At the *Hardware View*, right-click the port. A pop-up menu appears.
  2. Select *Reset Port*. A **This operation will cause a link reset to be sent to the attached device** message displays.
  3. Click *OK*. The port resets.
- b. Perform an external loopback test for all ports that were reset ([External Loopback Test \(Management Server\)](#) on page 4-32).

Did resetting ports solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**



## 15

An electronic circuit breaker on the port card may have tripped. To reset the circuit breaker, partially remove and reseat the port card for which external loopback tests failed ([RRP: Port Module Card \(UPM and XPM\)](#) on page 5-10).

- a. Unseat and disconnect the port card from the backplane. Unseat the card only, do not remove it from the director chassis.
- b. Reseat the port card in the backplane.
- c. Perform an external loopback test on the port card ([External Loopback Test \(Management Server\)](#) on page 4-32).

Did reseating the port card solve the problem?

**NO**      **YES**

↓      The director appears operational. **Exit MAP.**

Go to [step 7](#).

## 16

An director port is unblocked and receiving the offline sequence (OLS) or not operational sequence (NOS) from an attached device.

Inform the customer that the attached device failed or is set offline, and to take the appropriate corrective action. **Exit MAP.**

## 17

Beaconing is enabled for the port.

- a. Consult the customer and next level of support to determine the reason port beaconing is enabled.
- b. Disable port beaconing.
  1. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
  2. Click the *Enable Beaconing* option. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

**YES**      **NO**

↓      The director appears operational. **Exit MAP.**

Go to [step 1](#).

## 18

The eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device in the Element Manager application.

From the *Hardware View*, click *Node List*. Note the *Port WWN* column. This is the WWN assigned to the port or Fibre Channel interface installed on the attached device.

- If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer name.
- If a nickname is assigned to the WWN, the nickname appears in place of the WWN.

The bound WWN must be entered in the form of a raw WWN format (**XX:XX:XX:XX:XX:XX:XX:XX**) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 19

A port has an invalid attachment. The information in the *Port Properties* dialog box specifies the reason ([Table 3-12](#)).

**Table 3-12    Port Properties, Invalid Attachment Reasons and Actions**

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed.	Go to <a href="#">step 20</a> .
Incompatible switch.	Go to <a href="#">step 21</a> .
External loopback plug connected.	Go to <a href="#">step 22</a> .
N-Port connection not allowed.	Go to <a href="#">step 20</a> .
Non-McDATA switch at other end.	Go to <a href="#">step 21</a> .
Unauthorized port binding WWN.	Go to <a href="#">step 18</a> .
Unresponsive node.	Go to <a href="#">step 24</a> .

**Table 3-12 Port Properties, Invalid Attachment Reasons and Actions**

Reason	Action
ESA security mismatch.	Go to <a href="#">step 28</a> .
Fabric binding mismatch.	Go to <a href="#">step 29</a> .
Authorization failure reject.	Go to <a href="#">step 24</a> .
Unauthorized switch binding WWN.	Go to <a href="#">step 30</a> .
Fabric mode mismatch.	Go to <a href="#">step 21</a> .
CNT WAN extension mode mismatch.	Go to <a href="#">step 31</a> .

## 20

The port connection conflicts with the configured port type. Either an expansion port (E\_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F\_Port) is incorrectly cabled to a fabric element (director or switch).

- At the management server *Hardware View*, click *Configure* and select *Ports*. The *Configure Ports* dialog box displays.
- Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.
- Select (click) the *Type* field and configure the port from the list box as follows:
  - Select fabric port (**F\_Port**) if the port is cabled to a device (node).
  - Select expansion port (**E\_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.
- Click *Activate* to save the configuration information and close the window.

Did reconfiguring the port type solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

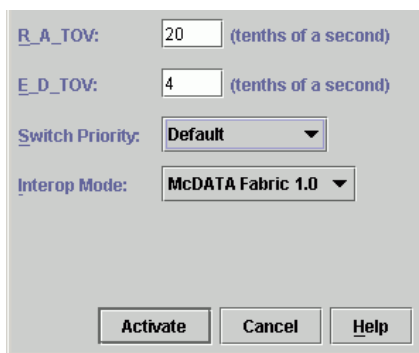
## 21

One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy McDATA director or switch at the incorrect Exchange Link Parameter (ELP) revision level.
- The director is configured for operation in **Open Fabric 1.0** mode and is connected to a non-McDATA switch at the incorrect ELP revision level.
- The director is configured for operation in **McDATA Fabric 1.0** mode and is connected to a non-McDATA switch.

Reconfigure the director operating mode:

- Ensure the director is set offline ([Set the Director Online or Offline](#) on page 4-43).
- At the *Hardware View*, click *Configure* and select *Operating Parameters* and *Fabric Parameters*. The *Configure Fabric Parameters* dialog box displays ([Figure 3-34](#)).



The dialog box is titled "Configure Fabric Parameters". It contains four configuration fields:

- R\_A\_TOV:** A text box with the value "20" and a label "(tenths of a second)".
- E\_D\_TOV:** A text box with the value "4" and a label "(tenths of a second)".
- Switch Priority:** A dropdown menu with "Default" selected.
- Interop Mode:** A dropdown menu with "McDATA Fabric 1.0" selected.

At the bottom of the dialog box are three buttons: "Activate", "Cancel", and "Help".

**Figure 3-34** Configure Fabric Parameters Dialog Box

- Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* list box.

- Select the **McDATA Fabric 1.0** option if the director is fabric-attached *only* to other McDATA directors or switches that are also operating in **McDATA Fabric 1.0** mode.
  - Select the **Open Fabric 1.0** option if the director is fabric-attached to directors or switches produced by other original equipment manufacturers (OEMs) that are open-fabric compliant.
- d. Click *Activate* to save the selection and close the window.

Did configuring the operating mode solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 22

A loopback (wrap) plug is connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

**YES NO**

↓ Contact the next level of support. **Exit MAP.**

## 23

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the director.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational and a device is attached, the green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Did removing the loopback plug solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 24

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security

violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

- a. Notify the customer the port will be blocked. Ensure the customer system administrator quiets Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port ([Blocking and Unblocking Ports](#) on page 4-46).
- c. Disconnect both ends of the fiber-optic cable.
- d. Clean the fiber-optic connectors ([Cleaning Fiber-Optic Components](#) on page 4-50).
- e. Reconnect the fiber-optic cable.
- f. Unblock the port ([Blocking and Unblocking Ports](#) on page 4-46).
- g. Monitor port operation for approximately five minutes.

Is the invalid attachment problem solved?

**YES    NO**

- ↓      The Fibre Channel link and director appear operational.  
**Exit MAP.**

## 25

Inspect both SBAR assemblies at the rear of the director. SBAR assembly LEDs can be inspected through the hexagonal cooling vents of the RFI shield.

Is the amber LED on an SBAR assembly illuminated but not blinking (beaconing)?

**YES    NO**

- ↓      The director appears operational. Go to [step 27](#).

## 26

An SBAR assembly failed and must be removed and replaced ([RRP: SBAR Assembly](#) on page 5-31).

- This procedure is concurrent and can be performed while director power is on.
- Perform the data collection procedure as part of FRU removal and replacement.

Did SBAR assembly replacement solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 27

Inspect and service the host bus adapters (HBAs), as necessary.

Did service of the HBAs solve the problem?

**NO YES**

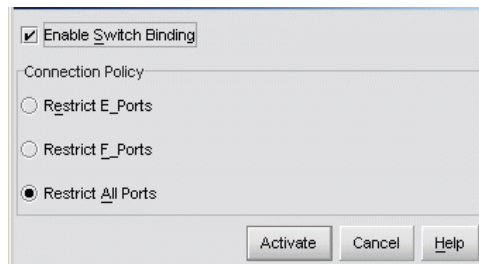
↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 28

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements.

- a. At the *Hardware View*, click *Configure* and select *Switch Binding* and *Change State*. The *Switch Binding - State Change* dialog box displays (Figure 3-35).



**Figure 3-35 Switch Binding - State Change Dialog Box**

- b. Ensure the *Enable Switch Binding* checkbox is enabled (checked) for both directors.
- c. Ensure the *Connection Policy* radio buttons are compatible for both directors.
- d. Click *Activate* for each director or switch. The switch binding feature is consistently enabled for both directors or switches.

Did configuring the switch binding parameters solve the problem?

**NO      YES**



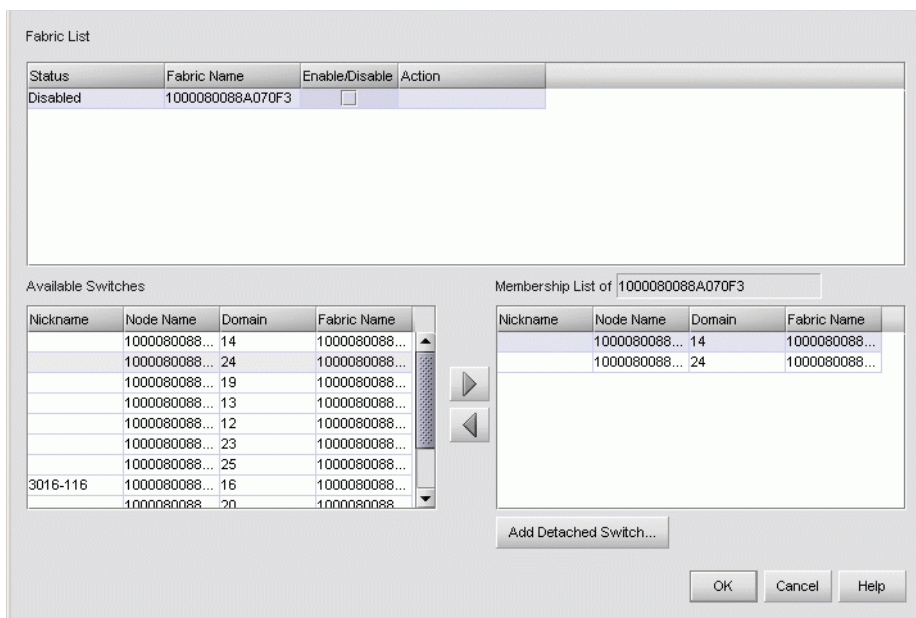
The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 29

A port connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both fabric elements.

- a. At the EFCM or SANavigator main window, select *Fabric Binding* from the *Configure* menu. The *Fabric Binding* dialog box displays (Figure 3-36).



**Figure 3-36 Fabric Binding Dialog Box**

- b. At the *Fabric List* section, ensure the *Enable/Disable* checkbox is enabled (checked) for the fabric containing both directors or switches.
- c. At the *Membership List of <Fabric Name>* section, update the membership list for both elements to ensure interswitch compatibility, then click **OK**. The fabric binding feature is consistently enabled for both directors or switches.



Did updating the fabric membership lists solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

**30**

A port connection is not allowed because of a switch binding mismatch. Switch membership lists must be compatible for both fabric elements.

- a. At the *Hardware View* for each director or switch, click *Configure* and select *Switch Binding* and *Edit Membership List*. The *Switch Binding - Membership List* dialog box displays (Figure 3-37).

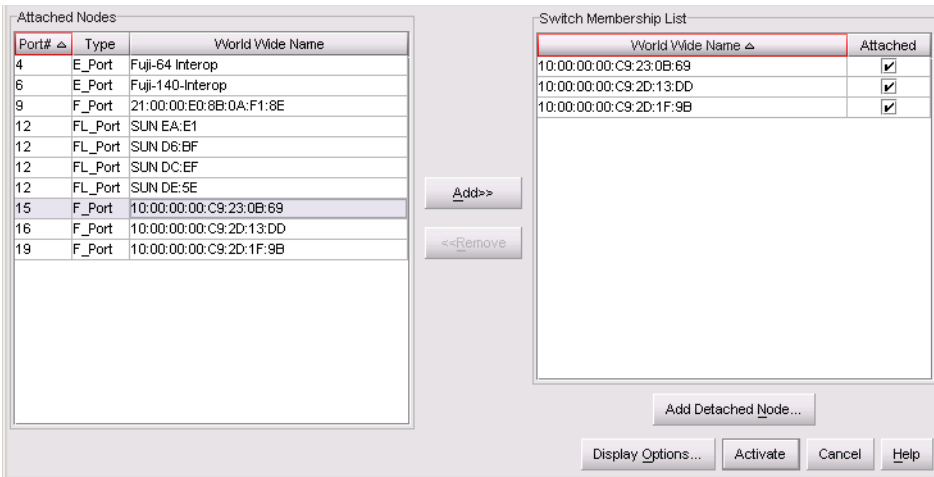


Figure 3-37 Switch Binding - Membership List Dialog Box

- b. At the *Switch Binding - Membership List* dialog box ensure the *Switch Membership List* is updated and correct for each director or switch, then click *Activate* for each director or switch. The switch binding feature is consistently enabled for both directors or switches.

Did updating the switch membership lists solve the problem?

**NO      YES**

↓      The director appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

### 31

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a director set to CNT WAN extension mode.

Contact McDATA support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow McDATA directors or switches to communicate with CNT UltraEdge WAN Gateways. **Exit MAP.**

### 32

The director and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

**NO      YES**



The Fibre Channel link and director appear operational. **Exit MAP.**

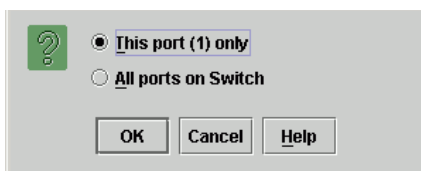
Go to [step 1](#).

### 33

A link incident message appeared in the *Link Incident Log* or in the *Link Incident* field of the *Port Properties* dialog box; or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI or FICON server attached to the director reporting the problem.

Clear the link incident for the port.

- a. At the *Hardware View*, right-click the port. A pop-up menu appears.
- b. Select *Clear Link Incident Alert(s)*. The *Clear Link Incident Alert(s)* dialog box displays ([Figure 3-38](#)).



**Figure 3-38** Clear Link Incident Alert(s)

- c. Select the **This port (n) only** radio button (where *n* is the port number) and click **OK**. The link incident clears.
- d. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES    NO**

- ↓      The problem is transient and the Fibre Channel link and director appear operational. **Exit MAP.**

## 34

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

- a. Notify the customer the port will be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port ([Blocking and Unblocking Ports](#) on page 4-46).
- c. Remove and replace the fiber-optic jumper cable.
- d. Unblock the port ([Blocking and Unblocking Ports](#) on page 4-46).

Was a corrective action performed?

**YES    NO**

- ↓      **Go to [step 36](#).**

## 35

Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES    NO**

- ↓      The Fibre Channel link and director appear operational. **Exit MAP.**

## 36

Clean fiber-optic connectors on the jumper cable.

- a. Notify the customer the port will be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
- b. Block the port ([Blocking and Unblocking Ports](#) on page 4-46).
- c. Disconnect both ends of the fiber-optic jumper cable.

- d. Clean the fiber-optic connectors (*Cleaning Fiber-Optic Components* on page 4-50).
- e. Reconnect the fiber-optic jumper cable.
- f. Unblock the port (*Blocking and Unblocking Ports* on page 4-46).
- g. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES    NO**

↓    The Fibre Channel link and director appear operational.  
**Exit MAP.**

## 37

Disconnect the fiber-optic jumper cable from the director port and connect the cable to a spare port.

Is a link incident reported at the new port?

**YES    NO**

↓    **Go to step 39.**

## 38

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

- a. Inspect and verify operation of the attached device.
- b. Repair the attached device if a failure is indicated.
- c. Monitor port operation for approximately five minutes.

Did the link incident recur?

**YES    NO**

↓    The attached device, Fibre Channel link, and director appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 39

The director port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port or port card degradation and a possible pending failure. **Go to step 6.**

## 40

A port card is not recognized by director firmware because the firmware version is not supported or the port card failed. Advise the

customer of the problem and determine the correct firmware version to download from the management server or customer-supplied server.

Download the firmware ([Download a Firmware Version to a Director](#) on page 4-63). Perform the data collection procedure after the download.

**Continue.**

## 41

Did the firmware download solve the problem?

**NO YES**

↓ The director appears operational. **Exit MAP.**

A port card failure is indicated. **Go to step 7.**

## 42

Does the SANpilot interface appear operational?

**NO YES**

↓ **Go to step 45.**

## 43

A **Page cannot be found, Unable to locate the server, HTTP 404 - file not found**, or other similar message appears. The message indicates the web browser PC cannot communicate with the director because:

- The director-to-PC Internet link could not be established.
- AC power distribution in the director failed, or AC power was disconnected.
- Both of the director CTP cards failed.

**Continue.**

## 44

Ensure the director reporting the problem is connected to facility AC power. Inspect the director for indications of being powered on:

- At the front bezel, an illuminated power LED (green) or system error LED (amber).
- An illuminated green LED on the active CTP card.
- At least one green **PWR OK** LED illuminated on a power supply.

- Audio emanations and airflow from cooling fans.

Does the director appear powered on?

**YES NO**



Analysis for an Ethernet link, AC power distribution, or dual CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-9](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

## 45

Inspect port card operational states at the SANpilot interface.

- At the *View* panel, click the *FRU Properties* tab. The *View* panel (*FRU Properties* tab) displays.
- Inspect the *Status* fields for port cards. Scroll down the *View* panel as necessary.

Does the *Status* field display a **Failed** message for a port card?

**NO YES**



A port card failure is indicated. **Go to [step 7](#).**

## 46

Inspect Fibre Channel port operational states at the SANpilot interface.

- At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays with port **0** highlighted in red.
- Click the port number (**0** through **139**) for which a failure is suspected to display properties for that port.
- Inspect the *Operational State* field. Scroll down the *View* panel as necessary.
- [Table 3-13](#) lists port operational states and associated MAP 0600 steps that describe fault isolation procedures.

**Table 3-13 MAP 600: Port Operational States and Actions (SANpilot)**

Operational State	Action
Offline	Go to <a href="#">step 16</a> .
Not Operational	Go to <a href="#">step 16</a> .
Port Failure	Go to <a href="#">step 6</a> .
Testing	Internal or external loopback test in process. <b>Exit MAP.</b>

Table 3-13 MAP 600: Port Operational States and Actions (SANpilot)

Operational State	Action
Invalid Attachment	Go to <a href="#">step 19</a> .
Link Reset	Go to <a href="#">step 32</a> .
Not Installed	Go to <a href="#">step 47</a> .

### 47

Install an SFP optical transceiver in the port receptacle (*RRP: Optical Transceiver (SFP and XFP)* on page 5-15).

- This procedure is concurrent and can be performed while director power is on.
- Verify the location of the failed port. [Figure 3-39](#) and [Figure 3-40](#) show UPM card numbers (**0** through **34**), port numbers (**00** through **139**), and bolded logical port addresses.
- Perform an external loopback test for the port as part of FRU removal and replacement (*External Loopback Test (Management Server)* on page 4-32).

### Exit MAP.

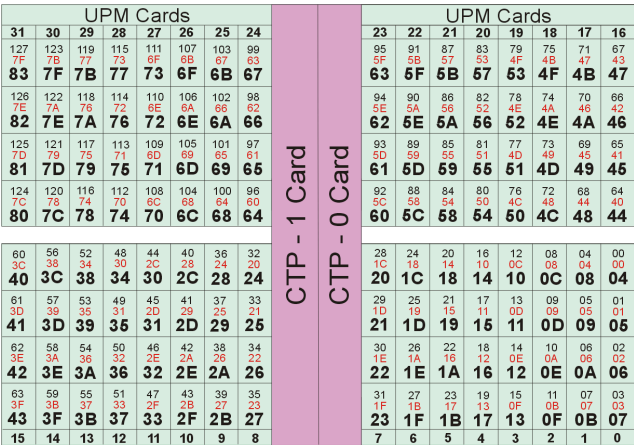


Figure 3-39 UPM Card Diagram (Front)

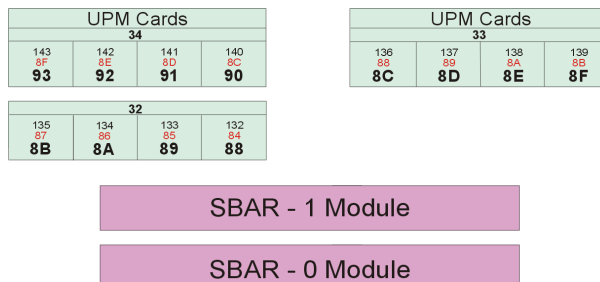


Figure 3-40 UPM Card Diagram (Rear)

## MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and E\_Port segmentation problems. Failure indicators include:

- An event code recorded at the *Intrepid 6140 Event Log* or the SANpilot event log.
- A segmentation reason associated with a Fibre Channel port at the SANpilot interface.
- A yellow triangle (attention indicator) appears over a port card graphic or at the alert panel of the *Hardware View*.
- A link incident message recorded in the *Link Incident Log* or *Port Properties* dialog box.

**1**

Was an event code **010, 011, 020, 021, 050, 051, 052, 060, 061, 062, 063, 070, 071, 072, 140, 142**, or **150** observed at the *Intrepid 6140 Event Log* (management server) or at the SANpilot event log?

**YES    NO**



**Go to [step 3](#).**



## 2

Table 3-14 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

**Table 3-14 MAP 700: Event Codes**

Event Code	Explanation	Action
010	Login server unable to synchronize databases.	Go to <a href="#">step 7</a> .
011	Login server database invalid.	Go to <a href="#">step 7</a> .
020	Name server unable to synchronize databases.	Go to <a href="#">step 7</a> .
021	Name server database invalid.	Go to <a href="#">step 7</a> .
050	Management server unable to synchronize databases.	Go to <a href="#">step 8</a> .
051	Management server database invalid.	Go to <a href="#">step 8</a> .
052	Management server internal error.	Go to <a href="#">step 8</a> .
060	Fabric controller unable to synchronize databases.	Go to <a href="#">step 9</a> .
061	Fabric controller database invalid.	Go to <a href="#">step 9</a> .
062	Maximum interswitch hop count exceeded.	Go to <a href="#">step 10</a> .
063	Received link state record too large.	Go to <a href="#">step 11</a> .
070	E_Port is segmented.	Go to <a href="#">step 12</a> .
071	Director is isolated.	Go to <a href="#">step 12</a> .
072	E_Port connected to unsupported switch.	Go to <a href="#">step 13</a> .
140	Congestion detected on an ISL.	Go to <a href="#">step 21</a> .
142	Low BB_Credit detected on an ISL.	Go to <a href="#">step 22</a> .
150	Zone merge failure.	Go to <a href="#">step 23</a> .

## 3

Is fault isolation being performed at the management server or customer-supplied server?

**YES NO**

↓ Fault isolation is being performed through the SANpilot interface. **Go to step 26.**

## 4

At the management server, does a yellow triangle (attention indicator) appear to overlay a port card graphic at the *Hardware View*?

**YES NO**

↓ The problem is transient and the director-to-fabric element connection appears operational. **Exit MAP.**

## 5

Inspect the port state and LED status for all ports with an attention indicator.

- a. At the *Hardware View*, double-click the port graphic with the attention indicator. The *Port Properties* dialog box displays.
- b. Inspect the *Operational State* field at the *Port Properties* dialog box.

Does the *Operational State* field indicate **Segmented E\_Port**?

**YES NO**

↓ Analysis for a port card failure or other link incident is not described in this MAP. Go to [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82. **Exit MAP.**

## 6

Inspect the *Segmentation Reason* field at the *Port Properties* dialog box. [Table 3-15](#) lists port segmentation reasons and associated steps that describe fault isolation procedures.

**Table 3-15 Port Segmentation Reasons and Actions (Management Server)**

Segmentation Reason	Action
Incompatible operating parameters.	Go to <a href="#">step 14</a> .
Duplicate domain IDs.	Go to <a href="#">step 15</a> .
Incompatible zoning configurations.	Go to <a href="#">step 16</a> .
Build fabric protocol error.	Go to <a href="#">step 17</a> .

**Table 3-15 Port Segmentation Reasons and Actions (Management Server) (*continued*)**

Segmentation Reason	Action
No principal switch.	Go to <a href="#">step 19</a> .
No response from attached switch.	Go to <a href="#">step 20</a> .
ELP retransmission failure timeout	Go to <a href="#">step 21</a>

## 7

A minor error occurred that caused fabric services databases to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 010** - Following a CTP card reset, the login server attempted to acquire a fabric server database copy from the other CTP card and failed.
- **Event code 011** - Following a CTP card failover, the login server database failed cyclic redundancy check (CRC) validation.
- **Event code 020** - Following a CTP card reset, the name server attempted to acquire a fabric server database copy from the other CTP card and failed.
- **Event code 021** - Following CTP card failover, the name server failed database CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the CD to McDATA for analysis.

**Exit MAP.**

## 8

A minor error occurred that caused management server database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the errors.

- **Event code 050** - Following CTP card reset, the management server attempted to acquire a database copy from the other CTP card and failed.
- **Event code 051** - Following CTP card failover, the management server database CRC validation.

- **Event code 052** - An internal operating error was detected by the management server subsystem.

All attached devices resume operation after management server login. Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

## 9

A minor error occurred that caused fabric controller databases to be re-initialized to an empty state. As a result, the director briefly lost interswitch link capability. The following list explains the errors.

- **Event code 060** - Following CTP card reset, the fabric controller attempted to acquire a database copy from the other CTP card and failed.
- **Event code 061** - Following CTP card failover, the fabric controller database failed CRC validation.

All interswitch links resume operation after CTP card reset or failover. Perform the data collection procedure and return the CD to McDATA for analysis. **Exit MAP.**

## 10

The Fabric Controller software detected a path to another director (or fabric element) in a multiswitch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

**NO      YES**

↓      The director and multiswitch fabric appear operational.  
**Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 11

The Fabric Controller software detected an:

- Intrepid 6064 Director in a multiswitch fabric that has more than 48 ISLs attached.
- Intrepid 6140 Director in a multiswitch fabric that has more than 70 ISLs attached.

- Other fabric element (other than an Intrepid 6140 Director) in a multiswitch fabric that has more than 32 ISLs attached.

Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems. Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no switch or switch elements have more than the proscribed number of ISLs.

Did fabric reconfiguration solve the problem?

**NO      YES**



The director and multiswitch fabric appear operational.

**Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 12

A **070** event code indicates an E\_Port detected an incompatibility with an attached director and prevented the directors from forming a multiswitch fabric. A segmented E\_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the director is isolated from all directors in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E\_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

- At the *Hardware View*, click Logs and select *Event Log*. The *Event Log* displays.
- Examine the first five bytes (**0** through **4**) of event data.
- Byte **0** specifies the director port number (**00** through **139**) of the segmented E\_port. Byte **4** specifies the segmentation reason (Table 3-16).

**Table 3-16    Byte 4, Segmentation Reasons, and Actions**

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to <a href="#">step 14</a> .
02	Duplicate domain IDs.	Go to <a href="#">step 15</a> .
03	Incompatible zoning configurations.	Go to <a href="#">step 16</a> .

Table 3-16 Byte 4, Segmentation Reasons, and Actions (*continued*)

Byte 4	Segmentation Reason	Action
04	Build fabric protocol error.	Go to <a href="#">step 17</a> .
05	No principal switch.	Go to <a href="#">step 19</a> .
06	No response from attached switch.	Go to <a href="#">step 20</a> .

## 13

A director E\_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. **Exit MAP.**

## 14

A director E\_Port segmented because the error detect time out value (E\_D\_TOV) or resource allocation time out value (R\_A\_TOV) is incompatible with the attached fabric element.

- a. Contact McDATA customer support or engineering personnel to determine the recommended E\_D\_TOV and R\_A\_TOV values for both directors or switches.
- b. Notify the customer both directors will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors or switches, and sets attached devices offline.
- c. Set both directors or switches offline ([Set the Director Online or Offline](#) on page 4-43).
- d. At the *Hardware View* for the first director or switch reporting the problem, click *Configure* and select *Operating Parameters* and *Fabric Parameters*. The *Configure Fabric Parameters* dialog box displays ([Figure 3-41](#)).

Figure 3-41 Configure Fabric Parameters Dialog Box

- e. Type the recommended E\_D\_TOV and R\_A\_TOV values, then click *Activate*.
- f. Repeat [step d](#) and [step e](#) at the *Hardware View* for the director attached to the segmented E\_Port (second director). Use the same E\_D\_TOV and R\_A\_TOV values.
- g. Set both directors or switches online ([Set the Director Online or Offline](#) on page 4-43).

Did the operating parameter change solve the problem and did both directors join through the ISL to form a fabric?

**NO      YES**



The directors, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 15

A director E\_Port segmented because two fabric elements had duplicate domain IDs.

- a. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each director or switch.
- b. Notify the customer both directors or switches will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the directors or switches, and sets attached devices offline.
- c. Set both directors or switches offline ([Set the Director Online or Offline](#) on page 4-43).

- d. At the *Hardware View* for the first director or switch reporting the problem, click *Configure* and select *Operating Parameters* and *Switch Parameters*. The *Configure Switch Parameters* dialog box displays (Figure 3-42).

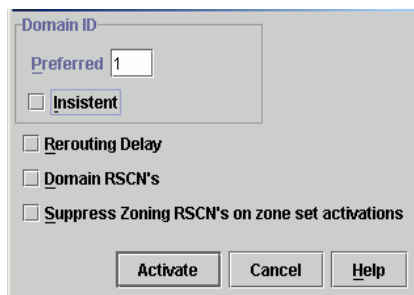


Figure 3-42 Configure Switch Parameters Dialog Box

- e. Type the customer-determined preferred domain ID value, then click *Activate*.
- f. Repeat [step d](#) and [step e](#) at the *Hardware View* for the director attached to the segmented E\_Port (second director or switch). Use a different preferred domain ID value.
- g. Set both directors or switches online ([Set the Director Online or Offline](#) on page 4-43).

Did the domain ID change solve the problem and did both directors join through the ISL to form a fabric?

**NO      YES**

- ↓      The directors, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

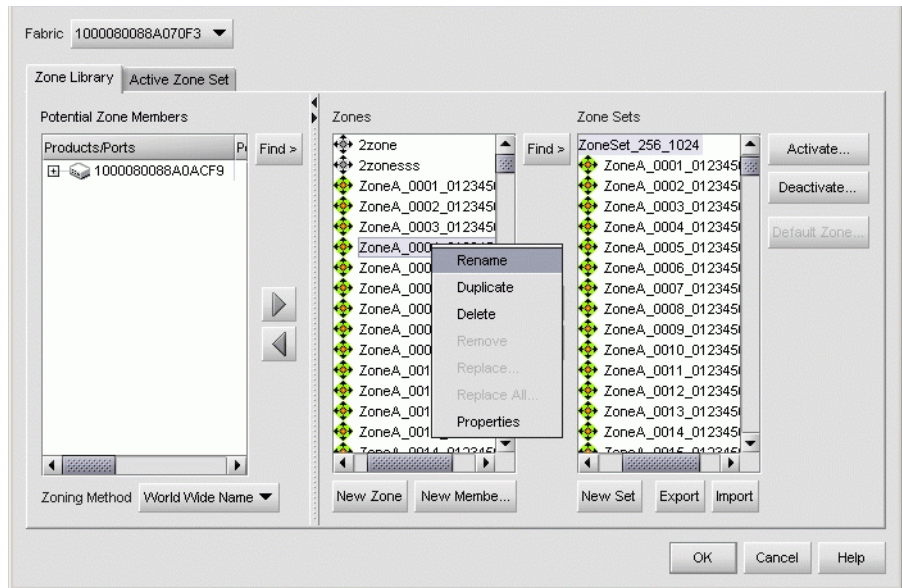
## 16

A director E\_Port segmented because two directors had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both directors, but the zones contain different members.

- a. Work with the system administrator to determine the desired zone name change for one of the affected directors. Zone names must conform to the following rules:

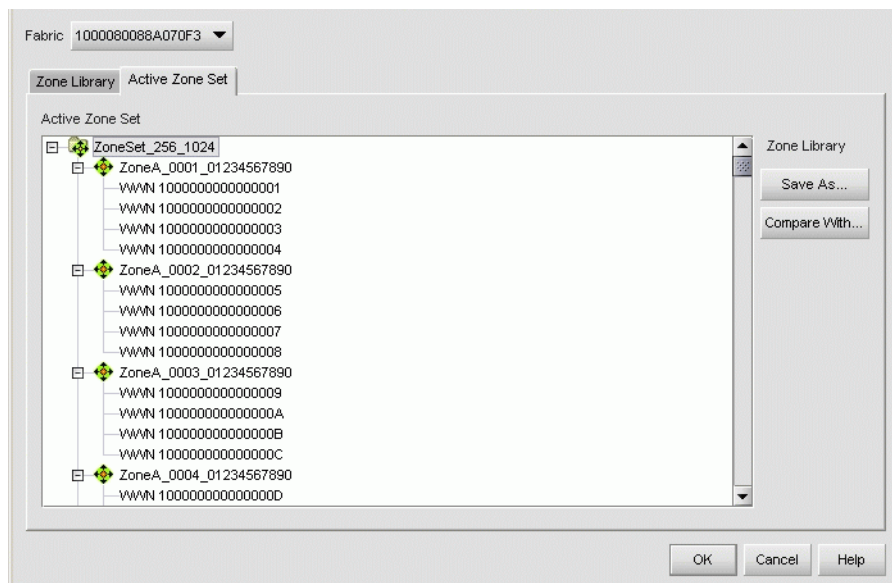


- The name must be 64 characters or fewer in length.
  - The first character must be a letter (**a** through **z**), upper or lower case.
  - Other characters are alphanumeric (**a** through **z** or **0** through **9**), dollar sign (\$), hyphen (-), caret (^), or underscore (\_).
- b. Close the Element Manager application (*Hardware View*). The SANavigator or EFCM main window (still active) displays.
  - c. At the EFCM or SANavigator main window physical map, right-click the blue background representing the fabric containing the switch reporting the problem. A pop-up menu appears.
  - d. Select the *Zoning* option from the menu. The *Zoning* dialog box displays with the *Zone Library* page open (Figure 3-43).



**Figure 3-43 Zoning Dialog Box (Zone Library Tab)**

- e. Click the *Active Zone Set* tab. The *Zoning* dialog box displays with the *Active Zone Set* page open (Figure 3-44).



**Figure 3-44 Zoning Dialog Box (Active Zone Set Tab)**

- f. Inspect zone names in the active zone set to determine the incompatible name.
- g. Modify the incompatible zone name as directed by the customer:
  1. At the *Zoning* dialog box, click the *Zone Library* tab. The dialog box returns to the *Zone Library* page ([Figure 3-43](#)).
  2. At the *Zones* field, right-click the zone name to be changed. A pop-up menu appears.
  3. Select the *Rename* option from the menu. The selected zone name remains highlighted in blue. Type the new zone name (specified by the customer), then click *OK* to activate the change and close the *Zoning* dialog box.

Did the zone name change solve the problem and did both director or switches join through the ISL to form a fabric?

**NO YES**



The director, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 17

A director E\_Port segmented because a build fabric protocol error was detected.

- a. Disconnect the fiber-optic jumper cable from the segmented E\_Port.
- b. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both directors join through the ISL to form a fabric?

**NO      YES**

- ↓      The directors, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

## 18

Initial program load (IPL) the director (*IML, IPL, or Reset the Director* on page 4-53).

Did the IPL solve the problem and did both directors join through the ISL to form a fabric?

**NO      YES**

- ↓      The director, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Perform the data collection procedure and contact the next level of support. **Exit MAP.**

## 19

A director E\_Port segmented because no director or switch in the fabric is capable of becoming the principal switch.

- a. Notify the customer the director will set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
- b. Set the director offline (*Set the Director Online or Offline* on page 4-43).
- c. At the Hardware View for the director, click Configure and select Operating Parameters and Fabric Parameters. The *Configure Fabric Parameters* dialog box displays (*Figure 3-34*).
- d. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default* (the default setting is *Default*. The switch priority value designates the fabric principal switch. The principal switch is

assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric directors and switches (including itself).

*Principal* is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means that the switch is incapable of becoming a principal switch. If all switches are set to *Principal* or *Default*, the switch with the highest priority and the lowest WWN becomes the principal switch.

At least one switch in a multiswitch fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment and the message *No Principal Switch* appears in the *Reason* field of the *Port Properties* dialog box.

- e. Set the director online ([Set the Director Online or Offline](#) on page 4-43).

Did the switch priority change solve the problem and did both directors join through the ISL to form a fabric?

**NO      YES**

- ↓      The directors, associated ISL, and multiswitch fabric appear operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 20

A director E\_Port segmented (at an operational director) because a response to a verification check indicates an attached director or switch is not operational.

- a. Perform the data collection procedure at the operational director and return the CD to McDATA for analysis. This information may assist in fault isolating the failed director.
- b. Go to [MAP 0000: Start MAP](#) on page 3-9 and perform fault isolation for the failed director.

**Exit MAP.**

## 21

A **140** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the directors or switches reporting the problem.
- Increase the ISL link speed between the directors or switches reporting the problem (from 1 Gbps to 2 Gbps or 10 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

**NO      YES**

↓      The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 22

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB\_Credit for a period of time that exceeded the configured low BB\_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the directors or switches reporting the problem.
- Increase the ISL link speed between the directors or switches reporting the problem (from 1 Gbps to 2 Gbps or 10 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB\_Credit condition?

**NO      YES**

↓      The ISL appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

## 23

A **150** event code indicates a zone merge failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

- a. At the *Hardware View*, click Logs and select *Event Log*. The *Event Log* displays.
- b. Examine the first 12 bytes (**0** through **11**) of event data.
- c. Bytes **0** through **3** specify the E\_Port number (**00** through **23**) reporting the problem. Bytes **8** through **11** specify the failure reason (Table 3-17).

**Table 3-17 Bytes 8 through 11 Failure Reasons and Actions**

Bytes 8 - 11	Failure Reason	Action
<b>01</b>	Invalid data length.	Go to <a href="#">step 24</a> .
<b>08</b>	Invalid zone set format.	Go to <a href="#">step 24</a> .
<b>09</b>	Invalid data.	Go to <a href="#">step 25</a> .
<b>0A</b>	Cannot merge.	Go to <a href="#">step 25</a> .
<b>F0</b>	Retry limit reached.	Go to <a href="#">step 24</a> .
<b>F1</b>	Invalid response length.	Go to <a href="#">step 24</a> .
<b>F2</b>	Invalid response code.	Go to <a href="#">step 24</a> .

## 24

A zone merge failed during ISL initialization. The following list explains the reason:

- **Failure reason 01** - An invalid data length condition caused an error in a zone merge frame.
- **Failure reason 08** - An invalid zone set format caused an error in a zone merge frame.
- **Failure reason F0** - A retry limit reached condition caused an error in a zone merge frame.

- **Failure reason F1** - An invalid response length condition caused an error in a zone merge frame.
- **Failure reason F2** - An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E\_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and was the resulting zone merge successful?

**NO YES**

↓ The merged zone appears operational. **Exit MAP.**

Perform the data collection procedure and return the CD to McDATA for analysis. Contact the next level of support. **Exit MAP.**

## 25

A zone merge failed during ISL initialization. The following list explains the reason:

- **Failure reason 09** - Invalid data caused a zone merge failure.
- **Failure reason 0A** - A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code.

- At the *Hardware View*, click Logs and select *Event Log*. The *Event Log* displays.
- Examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform the data collection procedure and return the CD to McDATA for analysis. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. **Exit MAP.**

## 26

Does the SANpilot interface appear operational?

**YES NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP card failure is not described in this MAP. Go to [MAP 0000: Start MAP on page 3-9](#). If this is the second time at this step, contact the next level of support. **Exit MAP.**

## 27

Inspect the Fibre Channel port segmentation reason at the SANpilot interface.

- At the *View* panel, click the *Port Properties* tab. The *View* panel (*Port Properties* tab) displays.
- Click the port number (**0** through **139**) of the segmented port.
- Inspect the *Segmentation Reason* field for the selected port.

Is the *Segmentation Reason* field blank or **N/A**?

**NO YES**

↓ The director ISL appears operational. **Exit MAP.**

The *Segmentation Reason* field displays a reason message.

[Table 3-18](#) lists segmentation reasons and associated steps that describe fault isolation procedures.

**Table 3-18 Segmentation Reasons and Actions (SANpilot)**

Segmentation Reason	Action
Incompatible operating parameters.	Go to <a href="#">step 14</a> .
Duplicate domain IDs.	Go to <a href="#">step 15</a> .
Incompatible zoning configurations.	Go to <a href="#">step 16</a> .
Build fabric protocol error.	Go to <a href="#">step 17</a> .
No principal switch.	Go to <a href="#">step 19</a> .
No response from attached switch.	Go to <a href="#">step 20</a> .



## MAP 0800: Server Hardware Problem Determination

This MAP describes isolation of hardware-related problems with the customer-supplied server communicating with the director through the management server or customer-supplied server running the SAN management application, or SANpilot interface.

The MAP provides only high-level fault isolation instructions. Refer to the documentation provided with the server for detailed problem determination and resolution.

To fault isolate software-related problems with the server, go to [MAP 0300: Server Application Problem Determination](#) on page 3-47.

To fault isolate director-to-server communication problems, go to [MAP 0400: Loss of Server Communication](#) on page 3-56.

### 1

Are you performing fault isolation at a customer-supplied server communicating with the director through the SANpilot interface?

**NO**      **YES**



The server and Internet browser application are not McDATA-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

### 2

Are you performing fault isolation at a customer-supplied, Unix-based server running the client SAN management application?

**NO**      **YES**



Unix-based servers are not McDATA-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

### 3

Are you performing fault isolation at one of the following servers?

- The management server running the Windows 2000 Professional operating system.

- A customer-supplied server running the client SAN management application and a Windows operating system (Windows 95, Windows 98, Windows 2000, Windows XP, or Windows NT 4.0).
- A customer-supplied server running the EFCM Lite application and the Windows-based operating system.

## YES NO

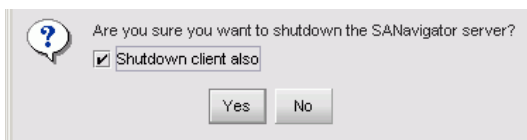


Analysis for the server failure is not described in this MAP. Contact the next level of support. **Exit MAP.**

## 4

At the server, close the EFCM Lite or SAN management application.

- Select *Shutdown* from the *SAN* menu. An *EFCM* or *SANavigator* Message dialog box displays (Figure 3-45).



**Figure 3-45 EFCM or SANavigator Message Dialog Box**

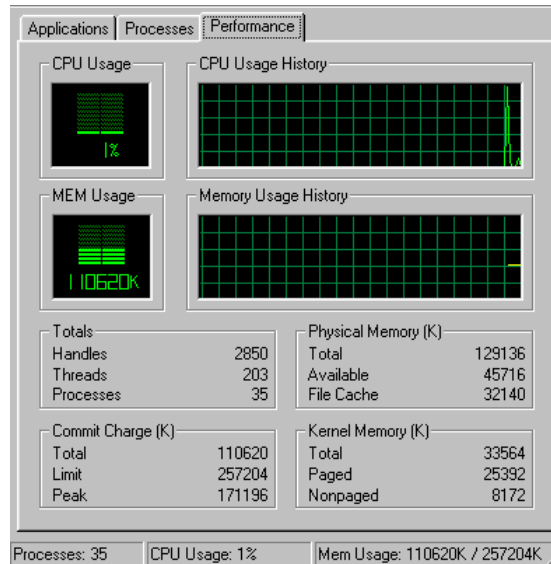
- Click *Yes* to close the SAN management application.
- Close any other applications.

**Continue.**

## 5

Inspect the available random access memory (RAM). The server must have a minimum of 128 megabytes (MB) of memory to run the Windows-based operating system and SAN management application.

- Right-click anywhere on the Windows task bar at the bottom of the desktop. A pop-up menu appears.
- Select *Task Manager*. The *Windows Task Manager* dialog box displays with the *Applications* page open. Click the *Performance* tab to open the *Performance* page (Figure 3-46).
- At the *Physical Memory (K)* portion of the dialog box, inspect the total amount of physical memory.
- Close the dialog box by clicking *Close (X)* at the upper right corner of the window.



**Figure 3-46 Windows Task Manager Dialog Box**

Does the computer have sufficient memory?

**YES NO**



A memory upgrade is required. Inform the customer of the problem and contact the next level of support. **Exit MAP.**

**6**

Reboot the server and perform system diagnostics.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-47).



**Figure 3-47 Shut Down Windows Dialog Box**

- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power ( $\Phi$ ) button on the LCD panel to power on the server and perform POSTs. During POSTs:
  1. The green LCD panel illuminates.
  2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
  3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-48):

**Boot from LAN?**  
**Press <Enter>**

**Figure 3-48 LCD Panel During Boot Sequence**

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.

- Fan 1, fan 2, fan 3, and fan 4 rotational speed.
- CPU temperature.
- Hard disk capacity.
- Virtual and physical memory capacity.

d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.

Did POSTs detect a problem?

**NO YES**



A computer hardware problem exists. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. **Exit MAP.**

## 7

After rebooting the server at the LCD panel, log on to the management server Windows 2000 desktop through a LAN connection to a browser-capable PC ([Access the Management Server Desktop](#) on page 2-26). The SAN management application starts and the *EFCM Log In* or *SANavigator Log In* displays ([Figure 3-49](#)).

**Figure 3-49 EFCM Log In or SANavigator Log In Dialog Box**

Did the *EFCM Log In* or *SANavigator Log In* dialog box display?

**YES NO**



**Go to [step 9](#).**

## 8

At the *EFCM Log In* or *SANavigator Log In* dialog box, type a user name and password, and click *Login*. The SAN management application opens and the EFCM or SANavigator main window displays (Figure 3-4).

Did the main window display and does the SAN management application appear operational?

**NO      YES**

↓      The server appears operational. **Exit MAP.**

## 9

Perform one of the following:

- If the server has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the server for instructions.
- If the server does not have standalone diagnostic test programs resident on fixed disk, **go to step 10.**

Did diagnostic test programs detect a problem?

**NO      YES**

↓      Refer to the supporting documentation shipped with the server for instructions to resolve the problem. **Exit MAP.**

## 10

Reboot the server.

- a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays (Figure 3-47).
- b. Select the *Shut Down* option from the list box and click *OK*. The management server powers down.
- c. Wait approximately 30 seconds and press the power (⏻) button on the LCD panel to power on the server and perform POSTs. During POSTs:
  1. The green LCD panel illuminates.
  2. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.

3. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 3-50):

The image shows a green rectangular box with a black border. Inside the box, the text "Boot from LAN?" is on the first line, and "Press <Enter>" is on the second line. Both lines are in a bold, black, sans-serif font.

**Figure 3-50 LCD Panel During Boot Sequence**

4. Ignore the message. After ten seconds, the server performs the boot sequence from BIOS. During the boot sequence, the server performs additional POSTs and displays the following operational information at the LCD panel:
  - Host name.
  - System date and time.
  - LAN 1 and LAN 2 IP addresses.
  - Fan 1, fan 2, fan 3, and fan 4 rotational speed.
  - CPU temperature.
  - Hard disk capacity.
  - Virtual and physical memory capacity.
- d. After successful POST completion, the LCD panel displays a **Welcome!!** message, then continuously cycles through and displays server operational information.
- e. After rebooting the server at the LCD panel, log on to the management server Windows 2000 desktop through a LAN connection to a browser-capable PC ([Access the Management Server Desktop](#) on page 2-26). The SAN management application starts and the *EFCM Log In* or *SANavigator Log In* dialog box displays (Figure 3-49).
- f. At the *EFCM Log In* or *SANavigator Log In* dialog box, type a user name and password, and click *Login*. The SAN management application opens and the EFCM or SANavigator main window displays (Figure 3-4).

Did the main window display and does the SAN management application appear operational?

**NO YES**



The server appears operational. **Exit MAP.**

## 11

Re-install the SAN management application ([Installing or Upgrading Software](#) on page 4-82).

Did the SAN management application install and open successfully?

**NO      YES**

↓      The server appears operational. **Exit MAP.**

## 12

Advise the customer and next level of support that the server hard drive should be restored to its original factory configuration. If the customer and support personnel do not concur, **go to step 13.**

- a. Format the server hard drive. Refer to supporting documentation shipped with the server for instructions.
- b. Install the Windows 2000 operating system and SAN management application ([Appendix E, Restore Management Server](#)).

Did the server hard drive format, and did the operating system and SAN management application install and open successfully?

**NO      YES**

↓      The server appears operational. **Exit MAP.**

## 13

Additional analysis for the failure is not described in this MAP. Contact the next level of support. **Exit MAP.**



This chapter describes repair-related procedures for the Intrepid 6140 Director and associated field- replaceable units (FRUs). The procedures are performed through the storage area network (SAN) management application (SANavigator or EFCM), Intrepid 6140 Element Manager application, or SANpilot interface. The following procedures are described:

- Obtaining log information.
- Obtaining port diagnostic information.
- Performing port diagnostic loopback tests.
- Performing channel wrap tests (FICON only).
- Swapping ports (FICON only).
- Collecting maintenance data.
- Setting the director online or offline.
- Blocking or unblocking Fibre Channel ports.
- Cleaning fiber-optic components.
- Powering the director on and off.
- Performing a director reset, initial machine load (IML), or initial program load (IPL).
- Managing firmware versions.
- Managing configuration data.
- Installing or upgrading software.

**NOTE:** Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, go to [MAP 0000: Start MAP](#) on page 3-9.

## Factory Defaults

[Table 4-1](#) lists the defaults for the passwords, and IP, subnet, and gateway addresses.

**Table 4-1 Factory-Set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

## Procedural Notes

**NOTE:** The screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

Note the following:

1. Before performing a procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, follow all electrostatic discharge (ESD) procedures, and **DANGER** and **CAUTION** statements.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
4. After completing a FRU replacement procedure, extinguish the amber system error light-emitting diode (LED) on the bezel at the top front of the director.

## Obtaining Log Information

The SAN management application, Intrepid 6140 Element Manager application, and SANpilot interface provide access to logs with information for administration, operation, and maintenance personnel.

- Logs accessed through the SAN management application (SANavigator or EFCM):
  - Audit Log.
  - Event Log.
  - Session Log.
  - Product Status Log.
  - Fabric Log.
- Logs accessed through the Element Manager application:
  - Intrepid 6140 Audit Log.
  - Intrepid 6140 Event Log.
  - Intrepid 6140 Hardware Log.
  - Intrepid 6140 Link Incident Log.
  - Intrepid 6140 Threshold Alert Log.
  - Intrepid 6140 Open Trunking Log.
- Logs accessed through the SANpilot interface:
  - Event Log.
  - Open Trunking Re-Route Log.
  - Link Incident Log.
  - Security Log
  - Audit Log
  - Fabric Log
  - Embedded Port Frame Log

## SAN Management Logs

To open a log from a SAN management application main window, select the *Logs* option from the *Monitor* menu, then click (select) the desired log option.

### Audit Log

To open the *Audit Log*, select the option from the *Monitor* and *Logs* menus. The log displays a history of user actions performed through the SAN management application. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.1 User Manual* (621-000013).

### Event Log

To open the *Event Log*, select the option from the *Monitor* and *Logs* menus. The log displays (Figure 4-1).

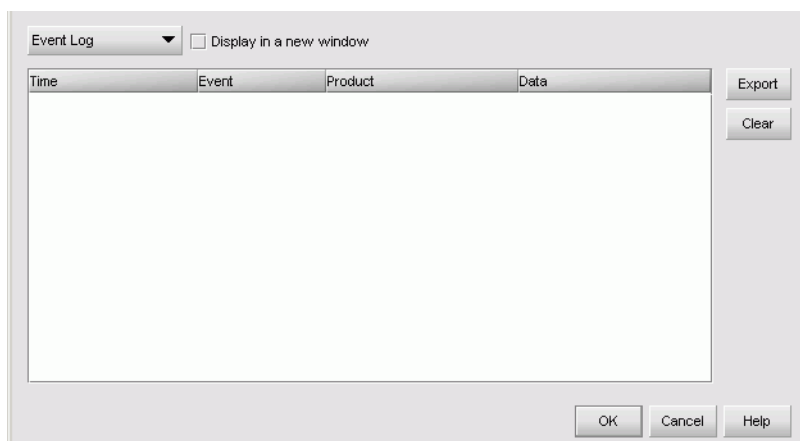


Figure 4-1 Event Log

The log displays SNMP trap events, client-server communication errors, and other problems recorded by the SAN management application. Information provided is generally intended for use by support personnel to fault isolate significant problems.

The log consists of the following columns:

- **Date/Time** - The date and time the event occurred.
- **Event** - An event number and brief description of the event. Include this information when reporting the event to customer support.
- **Product** - The product associated with the event and configured name or internet protocol (IP) address associated with the instance are displayed.

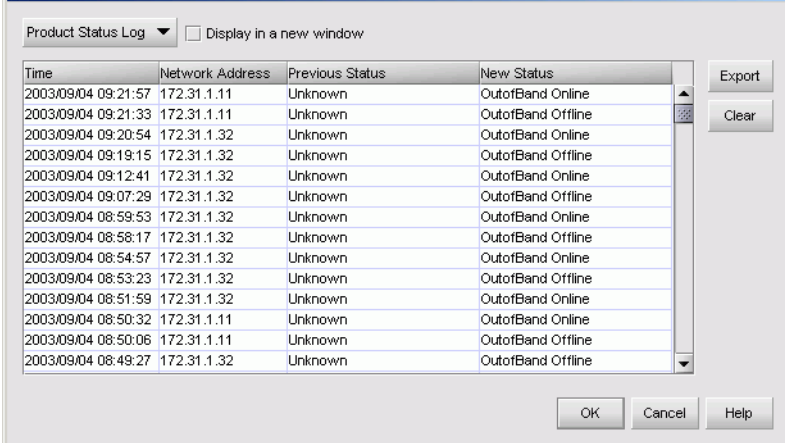
- **Data** - Additional event data for fault isolation. Include this information when fault isolating a call-home problem, or include the information when reporting an event to customer support.

### Session Log

To open the *Session Log*, select the option from the *Monitor* and *Logs* menus. The log displays a session (login and logout) history for the SAN management application. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.1 User Manual* (621-000013).

### Product Status Log

To open the *Product Status Log*, select the option from the *Monitor* and *Logs* menus. The log displays (Figure 4-2).



The screenshot shows a window titled "Product Status Log" with a checkbox "Display in a new window". It contains a table with four columns: Time, Network Address, Previous Status, and New Status. The table lists 16 entries of status changes between "Unknown" and "OutOfBand Offline" or "Online" for various network addresses. On the right side of the table are "Export" and "Clear" buttons. At the bottom right are "OK", "Cancel", and "Help" buttons.

Time	Network Address	Previous Status	New Status
2003/09/04 09:21:57	172.31.1.11	Unknown	OutOfBand Online
2003/09/04 09:21:33	172.31.1.11	Unknown	OutOfBand Offline
2003/09/04 09:20:54	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 09:19:15	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 09:12:41	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 09:07:29	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:59:53	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:58:17	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:54:57	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:53:23	172.31.1.32	Unknown	OutOfBand Offline
2003/09/04 08:51:59	172.31.1.32	Unknown	OutOfBand Online
2003/09/04 08:50:32	172.31.1.11	Unknown	OutOfBand Offline
2003/09/04 08:50:06	172.31.1.11	Unknown	OutOfBand Online
2003/09/04 08:49:27	172.31.1.32	Unknown	OutOfBand Offline

**Figure 4-2 Product Status Log**

The log reflects the previous and current status of the director, and indicates the instance of a Intrepid 6140 Element Manager application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification.

The log consists of the following columns:

- **Date/Time** - The date and time the director status change occurred.
- **Network Address** - The IP address or configured name of the director. This address or name corresponds to the address or name displayed under the product icon at the physical map.

- **Previous Status** - The status of the director prior to the reported status change (*Operational, Degraded, Failed, OutofBand Online, or Unknown*). An *Unknown* status indicates the SAN management application cannot communicate with the director.
- **New Status** - The status of the director after the reported status change (*Operational, Degraded, Failed, OutofBand Online, or Unknown*).

### Fabric Log

To open the *Fabric Log*, select the option from the *Monitor* and *Logs* menus. The log reflects the time and nature of changes made to a managed fabric. This information is useful for system administrators and users. For a log description, refer to the *SANavigator Software Release 4.1 User Manual* (621-000013).

### Element Manager Logs

To open a log from the Element Manager application, select the *Logs* menu at any view, then click (select) the desired log option.

#### Intrepid 6140 Audit Log

To open the *Intrepid 6140 Audit Log*, select the *Audit Log* option from the *Logs* menu at the *Hardware View, Port List View, Node List View, Performance View, or FRU List View*. The log displays a history of user actions performed through the Element Manager application or a simple network management protocol (SNMP) management workstation. This information is useful for system administrators and users. For a log description and an explanation of button functions, refer to the *McDATA Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153).

#### Intrepid 6140 Event Log

To open the *Intrepid 6140 Event Log*, select the *Event Log* option from the *Logs* menu at the *Hardware View, Port List View, Node List View, Performance View, or FRU List View*. The log displays (Figure 4-3).

Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

Export... Clear Refresh Close Help

Figure 4-3 Intrepid 6140 Event Log

The log displays a history of director events, such as degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and management server-to-director communication problems. The information is useful to maintenance personnel for fault isolation and repair verification.

The log contains the following columns:

- **Date/Time** - The date and time the event occurred.
- **Event** - The three-digit event code associated with the event. See [Appendix B, Event Code Tables](#) for an explanation of event codes.
- **Description** - A brief description of the event.
- **Severity** - The severity of the event (*Informational, Minor, Major, or Fatal*).
- **FRU-Position** - An acronym representing the FRU type, followed by a number representing the FRU chassis position. FRU acronyms are:
  - **BKPLNE** - backplane.
  - **CTP** - control processor (CTP) card.
  - **SBAR** - serial crossbar (SBAR) card.
  - **UPM** - universal port module (UPM) card.
  - **XPM** - 10 Gbps port module (XPM) card.
  - **PM** - port module (designation before a port module is identified as an FPM, UPM, or XPM type)
  - **FAN** - fan module.
  - **PWR** - power supply.

The chassis (slot) position for a nonredundant FRU is **0**. The chassis positions for redundant FRUs are **0** and **1**. The chassis positions for port cards are **0** through **34** inclusive.

- **Event Data** - Up to 32 bytes of supplementary event data (if available) in hexadecimal format. See [Appendix B, Event Code Tables](#) for an explanation of the supplementary event data.

## Intrepid 6140 Hardware Log

To open the Intrepid 6140 *Hardware Log*, select the *Hardware Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-4).

Date/Time ▲	FRU	Position	Action	Part Number	Serial Number
2003/09/03 14:48:21	Power	1	Inserted		
2003/09/03 14:48:05	Power	1	Removed		

Export...
Clear
Refresh
Close
Help

**Figure 4-4** Intrepid 6140 Hardware Log

The log displays a history of FRU removals and replacements (insertions) for the director. The information is useful to maintenance personnel for fault isolation and repair verification.

The log contains the following columns:

- **Date/Time** - The date and time the FRU was inserted or removed.
- **FRU** - An acronym representing the FRU type. FRU acronyms are:
  - **BKPLNE** - backplane.
  - **CTP** - CTP card.
  - **SBAR** - SBAR card.
  - **UPM** - UPM card.
  - **XPM** - XPM card.
  - **PM** - port module
  - **FAN** - fan module.
  - **PWR** - power supply.
- **Position** - A number representing the FRU chassis position. The chassis (slot) position for a nonredundant FRU is **0**. The chassis positions for redundant FRUs are **0** and **1**. The chassis positions for port cards are **0** through **34** inclusive.
- **Action** - The action performed (*Inserted* or *Removed*).
- **Part Number** - The part number of the inserted or removed FRU.
- **Serial Number** - The serial number of the inserted or removed FRU.



## Intrepid 6140 Link Incident Log

To open the Intrepid 6140 *Link Incident Log*, select the *Link Incident Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-5).

Date/Time ▲	port	Link Incident
2003/09/03 14:59:10	9	NOS Received
2003/09/03 14:59:04	11	NOS Received
2003/09/03 14:58:37	9	NOS Received

Export...
Clear
Refresh
Close
Help

E

**Figure 4-5** Intrepid 6140 Link Incident Log

The log displays a history of Fibre Channel link incidents (with associated port numbers) for the director. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E\_Port) segmentation problems) and repair verification.

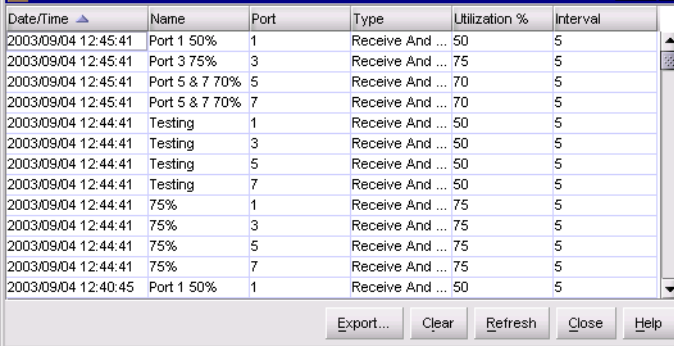
The log contains the following columns:

- **Date/Time** - The date and time the link incident occurred.
- **Port** - The port number (0 through 139 inclusive) that reported the link incident.
- **Link Incident** - A brief description of the link incident. Problem descriptions include:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Link failure - loss of signal or loss of synchronization.
  - Link failure - not-operational primitive sequence received.
  - Link failure - primitive sequence timeout.
  - Link failure - invalid primitive sequence received for current link state.

See [MAP 0600: Port Card Failure and Link Incident Analysis](#) on page 3-82 or [MAP 0700: Fabric, ISL, and Segmented Port Problem Determination](#) on page 3-104 for corrective actions in response to these link incident messages.

## Intrepid 6140 Threshold Alert Log

To open the Intrepid 6140 *Threshold Alert Log*, select the *Threshold Alert Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-6).



Date/Time	Name	Port	Type	Utilization %	Interval
2003/09/04 12:45:41	Port 1 50%	1	Receive And ...	50	5
2003/09/04 12:45:41	Port 3 75%	3	Receive And ...	75	5
2003/09/04 12:45:41	Port 5 & 7 70%	5	Receive And ...	70	5
2003/09/04 12:45:41	Port 5 & 7 70%	7	Receive And ...	70	5
2003/09/04 12:44:41	Testing	1	Receive And ...	50	5
2003/09/04 12:44:41	Testing	3	Receive And ...	50	5
2003/09/04 12:44:41	Testing	5	Receive And ...	50	5
2003/09/04 12:44:41	Testing	7	Receive And ...	50	5
2003/09/04 12:44:41	75%	1	Receive And ...	75	5
2003/09/04 12:44:41	75%	3	Receive And ...	75	5
2003/09/04 12:44:41	75%	5	Receive And ...	75	5
2003/09/04 12:44:41	75%	7	Receive And ...	75	5
2003/09/04 12:40:45	Port 1 50%	1	Receive And ...	50	5

Buttons: Export... Clear Refresh Close Help

Figure 4-6 Intrepid 6140 Threshold Alert Log

The log provides details of the threshold alert notifications. The log contains the following columns:

- **Date/Time** - The date and time stamp for when the alert occurred.
- **Name** - The name for the alert as configured through the *Configure Threshold Alerts* dialog box.
- **Port** - The port number where the alert occurred.
- **Type** - The type of alert: transmit (Tx) or receive (Rx).
- **Utilization %** - The percent usage of traffic capacity. This setting constitutes the threshold value and is configured through the *Configure Threshold Alerts* dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port capacity.
- **Interval** - The time interval during which the throughput is measured and an alert can generate. This is set through the *Configure Threshold Alerts* dialog box.

## Intrepid 6140 Open Trunking Log

To open the Intrepid 6140 *Open Trunking Log*, select the *Open Trunking Log* option from the *Logs* menu at the *Hardware View*, *Port List View*, *Node List View*, *Performance View*, or *FRU List View*. The log displays (Figure 4-7).

Date/Time ▲	Receive Port	Target Domain	Old Exit Port	New Exit Port
Thu Aug 28 13... 0	1	1	2	3
Thu Aug 28 13... 1	2	2	3	4
Thu Aug 28 13... 2	3	3	4	5
Thu Aug 28 13... 3	4	4	5	6
Thu Aug 28 13... 4	5	5	6	7

Export... Clear Refresh Close Help

**Figure 4-7 Intrepid 6140 Open Trunking Log**

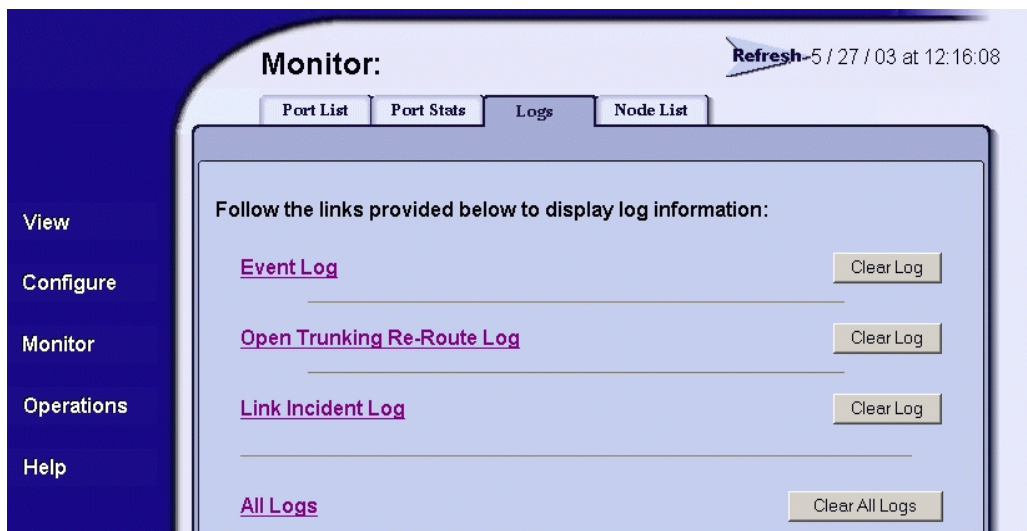
The log displays ISL congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed director.

The log contains the following columns:

- **Date/Time** - The date and time the re-route action occurred.
- **Receive Port** - The director port number (decimal) used for receiving Fibre Channel traffic after the re-route action.
- **Target Domain** - The domain ID (decimal) of the target device to which Fibre Channel traffic from the director was rerouted.
- **Old Exit Port** - The director port number (decimal) used for transmitting Fibre Channel traffic before the re-route action.
- **New Exit Port** - The director port number (decimal) used for transmitting Fibre Channel traffic after the re-route action.

## SANpilot Logs

To open a SANpilot log, click the *Logs* tab at the *Monitor* panel. The *Monitor* panel opens with the *Logs* page displayed ([Figure 4-8](#)).



**Figure 4-8 SANpilot Logs**

The *Logs* tab provides links to the following logs:

- Event Log - A listing of messages generated by the product regarding errors and events. The four levels of events indicate an increasing level of severity, from Informational to Severe.
- Open Trunking Re-Route Log - A log of open trunking re-route actions made by the product.
- Link Incident Log - A log of link incidents that have occurred.
- Security Log - List of security incidents that have occurred.
- Audit Log - List of events tracked for auditing purposes.
- Fabric Log - List of events associated with the Fabric.
- Embedded Port Frame Log - List of cumulative events.
- All Logs - collects the information for each log into a single text page.

---

**NOTE:** For details on the logs, review the *SANpilot User Manual*.

---

Each log contains a link that brings the user to a page of ASCII text that reflects the log information present on the machine at that moment. The log displayed is a snapshot of the current log

information. Log entries are displayed in the order in which they occurred, with most recent entries listed first. Each log also contains a *Clear Log* button that is used to clear all the entries in the log.

At the *Logs* page:

- Select (double-click) a log title to open and view the contents of the associated log, or
- Select (double-click) the *All Logs* title to open and simultaneously view the contents of all logs.

The *Logs* page provides a *Clear Log* button for each log. Click the button to delete all entries for the associated log. The *Logs* page also provides a *Clear All Logs* button. Click the button to delete all entries in all logs.

## Obtaining Port Diagnostic Information

Fibre Channel port diagnostic information can be obtained by:

- Inspecting port LEDs at the port card faceplates or emulated port LEDs at the management server *Hardware View*.
- Inspecting parameters at the management server (Intrepid 6140 Element Manager application).
- Inspecting parameters at the SANpilot interface.

### Port LEDs

To obtain port operational information, inspect port LEDs at the director port card faceplate or the emulated port LEDs at the management server *Hardware View*. These port operational states are defined in [Table 4-2](#).

Table 4-2 Port Operational States

Port State	Green LED	Amber LED	Alert Symbol	Description
Online	On	Off	None	An attached device is connected to the director and ready to communicate, or is communicating with other attached devices. If the port remains online, the green port LED remains illuminated. At the director port card, the green LED blinks when there is Fibre Channel traffic through the port.

Table 4-2 Port Operational States (*continued*)

Port State	Green LED	Amber LED	Alert Symbol	Description
Offline	Off	Off	None	The director port is blocked and transmitting the offline sequence (OLS) to the attached device.
	Off	Off	Yellow Triangle	The director port is unblocked and receiving the OLS, indicating the attached device is offline.
Beaconing	Off or On	Blinking	Yellow Triangle	The port is beaconing. The amber port LED blinks once every two seconds to enable users to locate the port.
Invalid Attachment	On	Off	Yellow Triangle	The director port has an invalid attachment state. The reasons for this state display in the <i>Reasons</i> field of the <i>Port Properties</i> dialog box.
Link Incident	Off	Off	Yellow Triangle	A link incident occurred on the port. The alert symbol appears at the <i>Port Card View</i> , <i>Port List View</i> , and <i>Hardware View</i> .
Link Reset	Off	Off	Yellow Triangle	The director and attached device are performing a link reset operation to recover the link connection. This is a transient state that should not persist.
No Light	Off	Off	None	No signal (light) is received by the director port. This is a normal condition when there is no cable attached to the port or when the attached device is powered off.
Inactive	On	Off	Yellow Triangle	The port is inactive. The reason appears in the <i>Reason</i> field at the <i>Port Properties</i> dialog box.
Not Installed	Off	Off	None	An optical transceiver is not installed in the director port.
Not Operational	Off	Off	Yellow Triangle	The director port is receiving the not operational sequence (NOS) from an attached device.
Port Failure	Off	On	Red and Yellow Blinking Diamond	The director port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	The E_Port is segmented, preventing two connected directors from joining and forming a multiswitch fabric. The reasons for the segmentation display in the <i>Reasons</i> field of the <i>Port Properties</i> dialog box.
Testing	Off	Blinking	Yellow Triangle	The port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	The port is performing an external loopback test.

## Management Server

To obtain port operational information at the management server (Intrepid 6140 Element Manager application), inspect parameters at the:

- *Port List View*.
- *Performance View*.
- *Port Properties* dialog box.
- *Port Technology* dialog box.

### Port List View

At the management server *Products View*, click the *Port List* tab. The *Port List View* displays (Figure 4-9). A row of information for each port (0 through 139 inclusive) appears.

Port #	Name	Block Config	State	Type	Operating Speed	Alert
0		Unblocked	No Light	GX_Port	Not Established	
1		Unblocked	Online	F_Port	1 Gig	▲
2		Unblocked	No Light	GX_Port	Not Established	
3		Unblocked	Online	F_Port	1 Gig	▲
4		Unblocked	No Light	GX_Port	Not Established	
5		Unblocked	Online	F_Port	1 Gig	▲
6		Unblocked	No Light	GX_Port	Not Established	
7		Unblocked	Online	F_Port	1 Gig	▲
8		Unblocked	No Light	GX_Port	Not Established	
9		Unblocked	Online	E_Port	1 Gig	▲
10		Unblocked	No Light	GX_Port	Not Established	
11		Unblocked	Online	E_Port	2 Gig	▲
12		Unblocked	No Light	GX_Port	Not Established	
13		Unblocked	No Light	GX_Port	Not Established	
14		Unblocked	No Light	GX_Port	Not Established	
15		Unblocked	No Light	GX_Port	Not Established	
16		Unblocked	No Light	GX_Port	Not Established	
17		Unblocked	No Light	GX_Port	Not Established	
18		Unblocked	No Light	GX_Port	Not Established	
19		Unblocked	No Light	GX_Port	Not Established	
20		Unblocked	No Light	GX_Port	Not Established	
21		Unblocked	No Light	GX_Port	Not Established	
22		Unblocked	No Light	GX_Port	Not Established	
23		Unblocked	No Light	GX_Port	Not Established	

**Figure 4-9 Port List View**

The view provides the following information:

- **#** - The director port number (0 through 139 inclusive).
- **Addr** - The director logical port address in hexadecimal format (FICON management style only).

- **Name** - The port name configured through the *Configure Ports* dialog box.
- **Block Config** - The port status (*Blocked* or *Unblocked*). Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the OLS.
- **State** - The port state (*Online, Offline, Testing, Beaconing, Invalid Attachment, Link Incident, Link Reset, No Light, Not Operational, Port Failure, Segmented E\_Port, or Testing*).
- **Type** - The type of port (*G\_Port, F\_Port, or E\_Port*).
- **Operating Speed** - The operating speed of the port (*Not Established, 2 Gbps, or 10 Gbps*).
- **Alert** - If link Incident (LIN) alerts are configured for the port through the *Configure Ports* dialog box, a yellow triangle appears in the column when a link incident occurs. A yellow triangle also appears if beaconing is enabled for the port. A red and yellow diamond appears if the port fails.

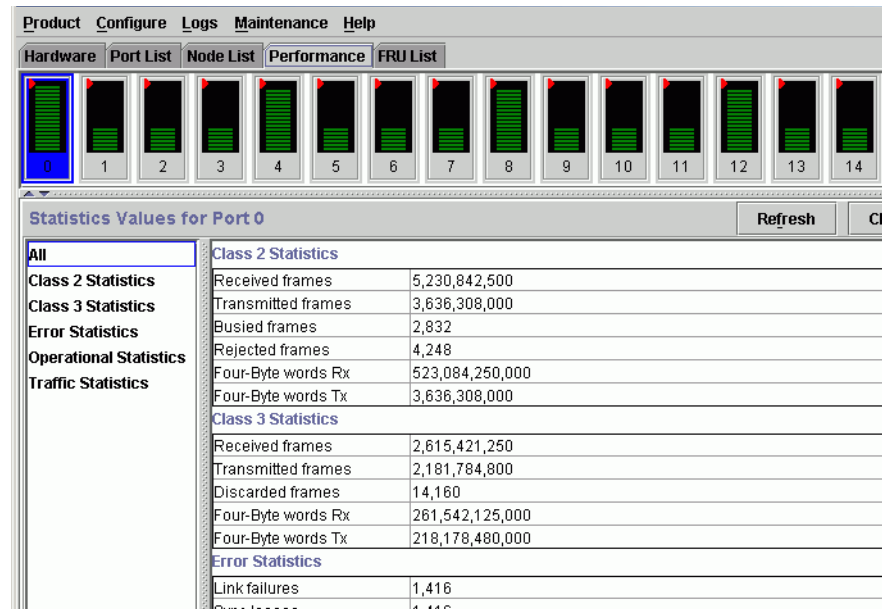
Click anywhere in a row to open the *Port Properties* dialog box (Figure 4-11). Right-click anywhere in a row for an installed port to open a menu to:

- Open the *Port Properties, Node Properties, or Port Technology* dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping (when the director is configured for FICON management style).
- Swap one Fibre Channel port address with another (when the director is configured for FICON management style).
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

## Performance View

At the management server, click the *Performance* tab. The *Performance View* displays (Figure 4-10).





**Figure 4-10 Performance View**

Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port, and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled).

Each port graph has 20 green-bar level indicators corresponding to 5% of the maximum throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar appears. A red indicator on each port bar graph (high-water mark) remains at the highest level the graph has reached since the port was set online. The indicator does not appear if the port is offline, and is reset to the bottom of the graph if the port detects a loss of light.

When the mouse cursor is passed over a port bar graph (flyover), the graph highlights with a blue border and an information pop-up displays the port operational state or WWN of the attached device. Click a port bar graph to display statistics values for the port. Right-click a port bar graph to open a pop-up menu to:

- Open the *Port Properties*, *Node Properties*, or *Port Technology* dialog boxes.

- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping (when the director is configured for FICON management style).
- Swap one Fibre Channel port address with another (when the director is configured for FICON management style).
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Class 2 statistics** - These entries provide information about Class 2 traffic, including:
  - Class 2 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Busied and rejected frames.
- **Class 3 statistics** - These entries provide information about Class 3 traffic, including:
  - Class 3 frames received and transmitted.
  - Four-byte words received and transmitted.
  - Discarded frames.
- **Error statistics** - The *Performance View* displays the following error statistics for the port:
  - **Link failures** - Link failures are recorded in response to an NOS, protocol timeout, or port failure. At the *Hardware View*, a yellow triangle appears to indicate a link incident, or a blinking red and yellow diamond appears to indicate a port failure.

- **Sync losses** - Synchronization losses are detected because an attached device was reset or disconnected from the port. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
- **Signal losses** - Signal losses are detected because an attached device was reset or disconnected from the port. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
- **Primitive sequence errors** - Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations. At the *Hardware View*, a yellow triangle appears to indicate a link incident.
- **Discarded frames** - Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the director.
- **Invalid transmission words** - Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.
- **CRC errors** - Received frames failed CRC validation, indicating the frames arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** - Received frames had frame delimiter errors, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
- **Address ID errors** - Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.
- **Frames too short** - Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the director port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- **Operational statistics** - These entries provide information about port operation, including:
  - Offline sequences received and transmitted.
  - Link resets received and transmitted.
  - LIPs generated and detected.
- **Traffic statistics** - These entries provide information about port traffic, including:
  - Percent link utilization (receive and transmit).
  - Fibre Channel frames received and transmitted.
  - Four-byte words received and transmitted.
  - Flows rerouted to and from ISLs.

### Port Properties Dialog Box

To open the *Port Properties* dialog box (Figure 4-11), double-click a port graphic at the *Hardware View* or a port row at the *Port List View*.

Port Number	2
Port Name	
Type	F_Port
Operating Speed	1 Gig
Port WWN	McDATA-20:06:08:00:88:00:21:00
Block Configuration	Unblocked
LIN Alerts Configuration	On
FAN Configuration	Off
Beaconing	Off
Link Incident	None
Operational State	Online
Reason	
Threshold Alert	

**Figure 4-11 Port Properties Dialog Box**

The dialog box provides the following information:

**NOTE:** If the Open Trunking feature is installed, an additional item, *Congested Threshold %*, appears in the Port Properties dialog box.

- **Port Number** - The director port number (0 through 139 inclusive).

- **Port Name** - The user-defined name or description for the port.
- **Type** - The Port type (*G\_Port*, *F\_Port*, or *E\_Port*) type of port (*G\_Port* if nothing is attached to the port, *F\_Port* if a device is attached to the port, and *E\_Port* if the port is connected to another director or switch as part of an ISL).
- **Operating Speed** - The operating speed of the port (*Not Established*, *2 Gbps*, or *10 Gbps*).
- **Port WWN** - The Fibre Channel WWN for the director port.
- **Block Configuration** - A user-configured state for the port (*Blocked* or *Unblocked*).
- **LIN Alerts Configuration** - A user-specified state for the port (*On* or *Off*), configured through the *Configure Ports* dialog box.
- **FAN Configuration** - A user-configured state for FAN configuration (*Enabled* or *Disabled*).
- **Beaconing** - User-specified for the port (*On* or *Off*). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
- **Link Incident** - If no link incidents are recorded, **None** appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field. Valid summaries are:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Link failure - loss of signal or loss of synchronization.
  - Link failure - not-operational primitive sequence received.
  - Link failure - primitive sequence timeout.
  - Link failure - invalid primitive sequence received for the current link state.
- **Operational State** - The state of the port (*Online*, *Offline*, *Beaconing*, *Invalid Attachment*, *Link Incident*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E\_Port*, or *Testing*). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.

- **Reason** - A summary appears describing the reason if the port state is *Segmented E\_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason field is blank or N/A.
- **Threshold Alert**- If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.

### Port Technology Dialog Box

To open the *Port Technology* dialog box (Figure 4-12), right-click a port graphic at the *Hardware View* or a port row at the *Port List View*, then select *Port Technology* from the pop-up menu.

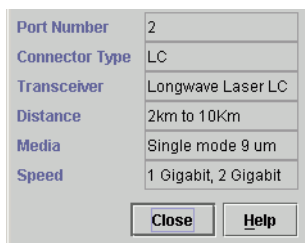


Figure 4-12 Port Technology Dialog Box

The dialog box provides the following information:

- **Port Number** - Director port number (0 through 139 inclusive).
- **Connector type** - Type of port connector (*LC*, *Unknown*, or *Internal Port*).
- **Transceiver** - Type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
- **Distance** - Port transmission distance (*Short*, *Intermediate*, *Long*, *Very Long*, or *Unknown*).
- **Media** - Type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
- **Speed** - Operating speed (*Not Established*, *2 Gbps*, or *10 Gbps*).

### SANpilot Interface

To obtain port operational information at the SANpilot interface, inspect parameters at the:

- *Monitor Panel - Port List* page.
- *Monitor Panel - Port Stats* page.
- *View panel - Port Properties* page.

**Port List Page** When the SANpilot interface opens, the *View* panel appears as the default. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed (Figure 4-13).

Port #	Name	Block Configuration	State	Type
0		Unblocked	Inactive	Gx Port
1		Unblocked	Inactive	Gx Port
2		Unblocked	Inactive	Gx Port
3		Unblocked	Inactive	Gx Port
4		Unblocked	Inactive	Gx Port
5		Unblocked	Inactive	Gx Port
6		Unblocked	Inactive	Gx Port
7		Unblocked	Inactive	Gx Port
8		Unblocked	Inactive	Gx Port
9		Unblocked	Inactive	Gx Port
10		Unblocked	Inactive	Gx Port
11		Unblocked	Inactive	Gx Port

**Figure 4-13 Monitor Panel (Port List Page)**

A row of information for each port (0 through 139 inclusive) appears. Each row consists of the following columns:

- **Port #** - The director port number.
- **Name** - The port name of 24 alphanumeric characters or less. The name typically characterizes the device or fabric element to which the port is attached.
- **Block Configuration** - Indicates if a port is blocked or unblocked. Blocking a port prevents the attached devices or fabric element from communicating. A blocked port continuously transmits the offline sequence (OLS).
- **State** - Port state (*Online, Offline, Not Installed, Inactive, Invalid Attachment, Link Reset, No Light, Not Operational, Port Failure, Segmented E\_Port, or Testing*).

- **Type** - The Port type (*G\_Port*, *F\_Port*, or *E\_Port*) type of port (*G\_Port* if nothing is attached to the port, *F\_Port* if a device is attached to the port, and *E\_Port* if the port is connected to another director or switch as part of an ISL).

### Port Stats Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, select the *Monitor* option at the left side of the panel. The *Monitor* panel opens with the *Port List* page displayed. Click the *Port Stats* tab. The *Monitor* panel displays with the *Port Stats* page selected (Figure 4-14).

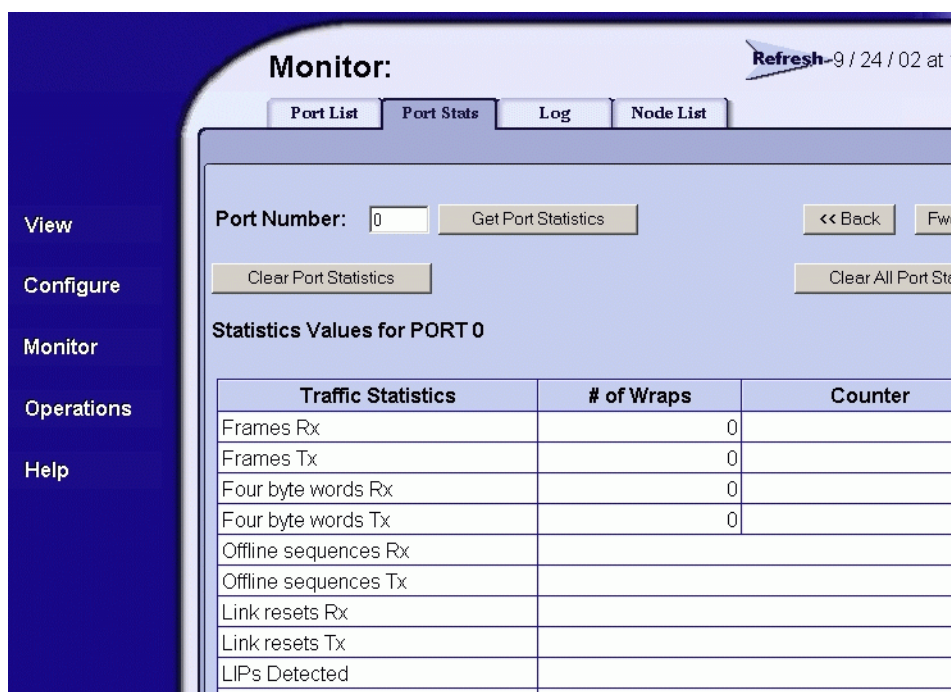


Figure 4-14 Monitor Panel (Port Stats Page)

### Troubleshooting Tip for Port Statistics

As a general rule, you should clear all the counters by selecting *Clear Port Stats* or *Clear All Port Stats* after you have resolved a problem. When troubleshooting, keep track of the time interval when errors accumulate to judge the presence and severity of a problem. (There is a link recovery hierarchy implemented in Fibre Channel to handle some level of “expected anomalies”.) For troubleshooting purposes, you want to focus on when the errors, as displayed in the *Counter* column, increment very quickly.



### Parts of Statistics Tables

The tables of statistics contain the following columns:

- **Statistics** - the type of statistic being tracked.
- **# of Wraps** - times the *Counter* value wraps, for statistics that grow rapidly. The maximum value that either the *Counter* or the *# of Wraps* can hold is  $2^{32}$ , or 4,294,967,296. Each time the *Counter* field reaches the maximum value of  $2^{32}$ , the wrap count is incremented by 1.
- **Counter** - the number of instances of the tracked item recorded since system initialization or the last time the counters were cleared.

### Traffic Transmit and Receive Statistics

The Traffic Statistics include these transmit and receive values.

- **Frames Rx** - The number of frames that the port has received.
- **Frames Tx** - The number of frames that the port has transmitted.
- **Four byte words Rx** - The number of words that the port has received.
- **Four byte words Tx** - The number of words that the port has transmitted.
- **Offline sequences Rx** - The number of offline sequences (OLS) received by this port.
- **Offline sequences Tx** - The number of offline sequences (OLS) transmitted by this port.
- **Link resets Rx** - The number of link reset protocol frames received by this port from the attached N\_Port.
- **Link resets Tx** - The number of link reset protocol frames transmitted by this port to the attached N\_Port.
- **Link utilization % Rx** - The current link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.
- **Link utilization % Tx** - The current link utilization for the port expressed as a percentage. On 1 Gbps links, ports can transmit or receive data at 100 MB per second. On 2 Gbps links, ports can transmit or receive data at 200 MB per second. Link utilization is calculated over one-second intervals.

For the Sphereon 4300 and Sphereon 4500 switches, the following statistics are also shown:

- **LIPs Detected** - A loop initialization primitive was detected, which means the loop was completed.
- **LIPs Generated** - A loop initialization primitive was created to initialize a loop.

### Error Statistics

The Error Statistics include these transmit and receive values:

- **Link failures** - The number of link failures recorded because a not operational sequence (NOS), protocol timeout, or port failure was detected.
- **Sync losses** - The number of loss-of-synchronizations detected because an attached device was reset or disconnected from the port.
- **Signal losses** - The number of loss-of-signal errors detected because the attached device was reset or disconnected from the port.
- **Primitive sequence errors** - The number of primitive sequence protocol errors received from an attached device, which indicates a Fibre Channel link-level protocol violation.
- **Discarded frames** - A received frame could not be routed and was discarded because the frame timed out due to an insufficient buffer-to-buffer credit, or the destination device was not logged into the product.
- **Invalid transmission words** - The number of invalid transmission words from an attached device. This indicates that a frame or primitive sequence arrived at the port corrupted.
- **CRC errors** - A received frame failed a cyclic redundancy check (CRC) validation, indicating the frame arrived at the port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure, a bad fiber-optic cable, or a poor cable connection.
- **Delimiter errors** - The number of times that the switch detected an unrecognized start-of-frame (SOF), an unrecognized end-of-frame (EOF) delimiter, or an invalid class of service. This indicates that the frame arrived at the switch's port corrupted. This corruption can be due to plugging/unplugging the link, bad

optics at either end of the cable, bad cable, or dirty or poor connections. Moving the connection around or replacing cables can isolate the problem.

- **Address ID errors** - A received frame had an unavailable or invalid Fibre Channel destination address, or an invalid Fibre Channel source address. This typically indicates the destination device is unavailable.
- **Frames too short** - A received frame exceeded the Fibre Channel frame maximum size or was less than the Fibre Channel minimum size, indicating the frame arrived at the switch's port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

### Class 2 Statistics

The Class 2 Statistics include these transmit and receive values:

- **Received Frames** - The number of Class 2 frames received by this F\_Port from its attached N\_Port.
- **Transmitted Frames** - The number of Class 2 frames transmitted by this F\_Port to its attached N\_Port.
- **4-byte words Rx** - The number of Class 2, 4-byte words received by the port.
- **4-byte words Tx** - The number of Class 2, 4-byte words transmitted by the port.
- **Busied Frames** - The number of F\_BSY frames generated by this F\_Port against Class 2 frames.
- **Rejected Frames** - The number of F\_RJT frames generated by this F\_Port against Class 2 frames.

### Class 3 Statistics

The Class 3 Statistics include these transmit and receive values:

- **Received Frames** - The number of Class 3 frames received by the F\_Port from its attached N\_Port.
- **Transmitted Frames** - The number of Class 3 frames transmitted by this F\_Port to its attached N\_Port.
- **Discarded Frames** - The number of Class 3 frames discarded (including multicast frames with bad Domain IDs).
- **4-byte words Rx** - The number of Class 3, 4-byte words received by the port.

### Open Trunking Statistics

- **4-byte words Tx** - The number of Class 3, 4-byte words transmitted by the port.

The Open Trunking Statistics include these transmit and receive values:

- **Flows rerouted to ISL** - The number of Fibre Channel traffic flows that were rerouted to this ISL from another ISL due to congestion. (This value increments only if the OpenTrunking feature is installed.)
- **Flows rerouted from ISL** - The number of Fibre Channel traffic flows that were rerouted from this ISL to another ISL due to congestion. (This value increments only if the OpenTrunking feature is install

---

### Port Properties Page

When the SANpilot interface opens, the *View* panel appears as the default panel. At the *View* panel, click the *Port Properties* tab. The *View* panel displays with the *Port Properties* page selected ([Figure 4-15](#)).

The screenshot shows a web interface for viewing port properties. On the left is a dark blue sidebar with menu items: View, Configure, Monitor, Operations, and Help. The main area has a header 'View:' with a 'Refresh' button and a timestamp '-9 / 24 / 02 at 11:'. Below the header are tabs: Switch, Port Properties (selected), FRU Properties, Unit Properties, Operating Parameters, and Fabric. The 'Port Properties' section includes a 'Port Number' input field set to '0', a 'Get Port Properties' button, and '<< Back' and 'Fwd >>' buttons. Below this is a table of port details.

Port Number	0
Port Name	
Type	Gx Port
Operating Speed	2 Gb/sec
Port WWN	20:04:08:00:88:00:07:3D
Block Configuration	Unblocked
Beaconing	Off
FAN Configuration	Enabled
Operational State	Inactive
Reason	Optics Speed Conflict
<b>Technology</b>	
Connector Type	LC
Transceiver	Shortwave Laser
Distance Capability	Intermediate
Media	Multi-Mode 50, 62.5 micrometer
Speed	1 Gb/sec

**Figure 4-15 View Panel (Port Properties Page)**

The *Port Properties* page displays information for one port. Values update only when the page opens for a selected port or the user selects *Get Port Properties*. The page defaults to port 0. Increment or decrement the port number displayed (0 through 139 inclusive) by clicking *Fwd>>* or *<<Back*. The page provides the following information:

- **Port Number** - The director port number.
- **Port Name** - The user-defined name or description for the port.
- **Type** - The Port type (*G\_Port*, *F\_Port*, or *E\_Port*) type of port (*G\_Port* if nothing is attached to the port, *F\_Port* if a device is attached to the port, and *E\_Port* if the port is connected to another director or switch as part of an ISL).

- **Operating Speed** - The operating speed (*Not Established, 2 Gbps, or 10 Gbps*).
- **Port WWN** - The Fibre Channel world wide name (WWN) for the port.
- **Block Configuration** - the user-configured state for the port (*Blocked or Unblocked*).
- **Beaconing** - The user-specified for the port (*On or Off*).
- **FAN Configuration** - The user-configured state for fabric address notification (FAN) configuration (*Enabled or Disabled*).
- **Operational State** - The port state (*Online, Offline, Not Installed, Inactive, Invalid Attachment, Link Reset, No Light, Not Operational, Port Failure, Segmented E\_Port, or Testing*).
- **Reason** - A summary appears describing the reason if the port state is *Segmented E\_Port, Invalid Attachment, or Inactive*. For any other port state, the reason is *N/A*.
- **Technology** - Information specific to the installed optical transceiver, including connector type, transceiver optics, data transmission distance, optical media (cable type), and transmission speed.

---

## Performing Port Diagnostic Loopback Tests

Port diagnostics consist of internal and external loopback tests. The tests are performed on any selected port at the management server (Intrepid 6140 Element Manager application) or at the SANpilot interface. The tests are:

- **Internal loopback test** - An internal loopback test checks port card circuitry, but does not check fiber-optic components of a port transceiver. The test is performed with a device attached to the port, but the test momentarily blocks the port and is disruptive to the attached device.
- **External loopback test** - An external loopback test checks port card circuitry, including fiber-optic components of a port transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a multimode or singlemode loopback plug must be inserted in the port receptacle.

## Internal Loopback Test (Management Server)

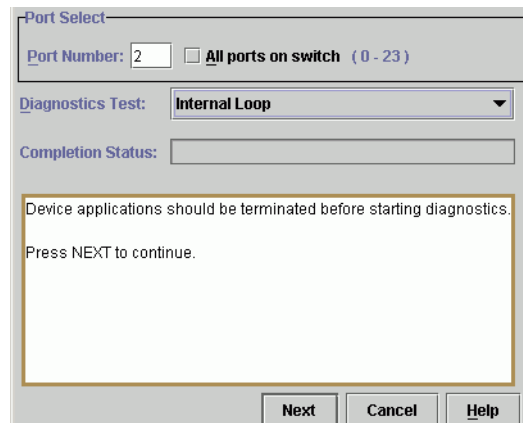
To perform an internal loopback at the management server (Intrepid 6140 Element Manager application):

1. Notify the customer a disruptive internal loopback test will be performed on a port or port card. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the port or port card, and sets attached devices offline.

**NOTE:** At the start of the loopback test, the port or port card can be online, offline, blocked, or unblocked.

**NOTE:** An optical transceiver (SFP or XFP) must be installed in the port during the test. A device can remain connected during the test.

2. At the management server, open the SAN management application (SANavigator or EFCM).
3. At the SAN management application physical map, right-click the product icon representing the director to be tested, then select *Element Manager* from the pop-up menu. The application opens.
4. Select the *Port Diagnostics* option from the *Maintenance* menu. The *Port Diagnostics* dialog box displays (Figure 4-16).



**Figure 4-16** Port Diagnostics Dialog Box

5. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
6. At the *Diagnostics Test* list box, select *Internal Loopback*.

7. Click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.
8. Click *Start Test*. The test begins and:
  - The *Start Test* button changes to a *Stop Test* button.
  - The message **Port xx: TEST RUNNING** appears, where *xx* is the port number. If a port card is tested, the message appears for all ports.
  - A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

As a port is tested, the amber LED flashes (beacons) and the green LED extinguishes (indicating the port is blocked).

---

**NOTE:** Click *Stop Test* at any time to abort the loopback test.

---

9. When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.
10. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
11. Reset the port:
  - a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
  - b. Select the *Reset Port* option. A *Message* message box displays, indicating a link reset operation will occur.
  - c. Click *OK*. The port resets.
12. Notify the customer the test is complete and the attached device can be set online.

---

### External Loopback Test (Management Server)

To perform an external loopback test at the management server (Intrepid 6140 Element Manager application):

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.

---

**NOTE:** At the start of the loopback test, the port or port card can be online, offline, blocked, or unblocked.

---



2. At the management server, open the SAN management application (SANavigator or EFCM).
3. At the SAN management application physical map, right-click the product icon representing the director to be tested, then select *Element Manager* from the pop-up menu. The application opens.
4. Disconnect the fiber-optic jumper cable from the port to be tested. If a port card will be tested, disconnect all fiber-optic jumper cables.

---

**ATTENTION!** If name server zoning is implemented by port number, ensure fiber-optic cables that are disconnected to perform the loopback test are reconnected properly. A cable configuration change disrupts zone operation and may incorrectly include or exclude a device from a zone.

---

5. Insert a loopback plug into the port.
  - If the port to be tested is shortwave laser, insert a multimode loopback plug into the port receptacle.
  - If the port to be tested is longwave laser, insert a singlemode loopback plug into the port receptacle.
  - If an entire port card will be tested, insert an appropriate loopback plug in all port receptacles.
6. Select the *Port Diagnostics* option from the *Maintenance* menu. The *Port Diagnostics* dialog box displays (Figure 4-16).
7. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
8. At the *Diagnostics Test* list box, select the *External Loop* option.
9. Click *Next*. At the *Port Diagnostics* dialog box, the message **Loopback plug(s) must be installed on ports being diagnosed** appears.
10. Verify a loopback plug is installed and click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.

11. Click *Start Test*. The test begins and:
  - a. The *Start Test* button changes to a *Stop Test* button.
  - b. The message **Port xx: TEST RUNNING** appears.
  - c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

---

**NOTE:** Click *Stop Test* at any time to abort the loopback test.

---

12. When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
13. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
14. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port.
15. Reset the port:
  - a. At the *Hardware View*, right-click the port graphic. A pop-up menu appears.
  - b. Select the *Reset Port* option. A *Message* message box displays, indicating a link reset operation will occur.
  - c. Click *OK*. The port resets.
16. Notify the customer the test is complete and the device can be reconnected to the director and set online.

---

### Internal Loopback Test (SANpilot Interface)

To perform an internal loopback at the SANpilot interface:

1. Notify the customer that a disruptive internal loopback test is to be performed. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the port, and sets the attached device offline.

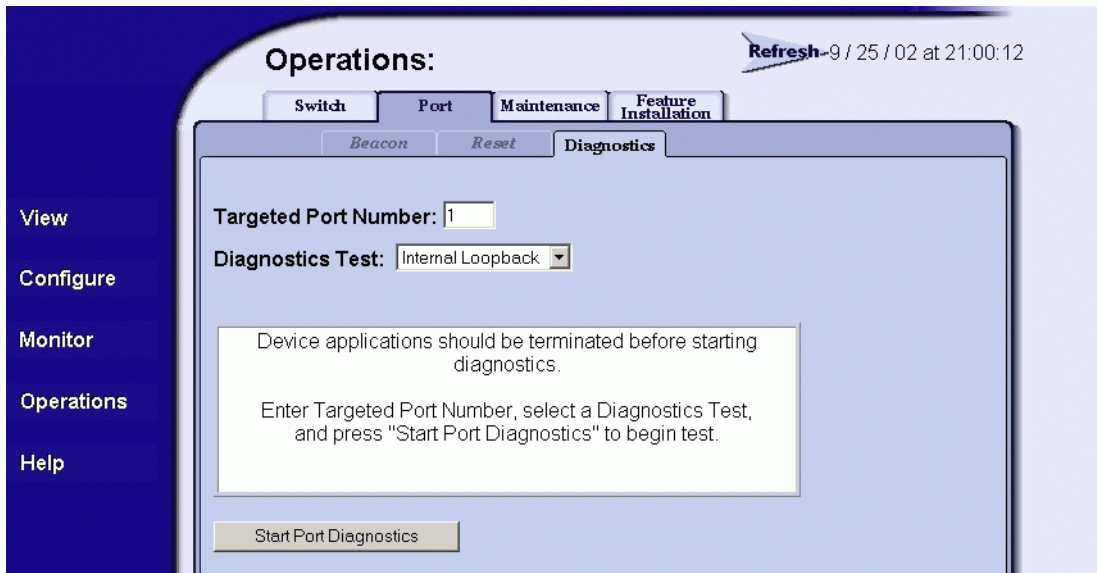
---

**NOTE:** An optical transceiver (SFP or XFP) must be installed in the port during the test. A device can remain connected during the test.

---

2. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.

3. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-17).



**Figure 4-17 Operations Panel (Port Page with Diagnostics Tab)**

4. Type the port number to be tested in the *Targeted Port Number* field.
5. At the *Diagnostics Test* list box, select the *Internal Loopback* option.
6. Click *Start Port Diagnostics*. The test begins and:
  - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.
  - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

---

**NOTE:** Click *Terminate Port Diagnostics* at any time to abort the loopback test.

---

7. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.
8. Reset the tested port:

- a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
  - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
  - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
9. Notify the customer the test is complete and the attached device can be set online.

---

### External Loopback Test (SANpilot Interface)

To perform an external loopback at the SANpilot interface:

1. Notify the customer that a disruptive external loopback test is to be performed and the attached device must be disconnected.
2. Disconnect the fiber-optic jumper cable from the port to be tested.
3. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
4. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
5. Click the *Port* and *Diagnostics* tabs. The *Port* page displays with the *Diagnostics* tab selected (Figure 4-17).
6. Type the port number to be tested in the *Targeted Port Number* field.
7. At the *Diagnostics Test* list box, select the *External Loopback* option.
8. Click *Start Port Diagnostics*. The test begins and:
  - a. The *Start Port Diagnostics* button changes to a *Terminate Port Diagnostics* button.
  - b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

---

**NOTE:** Click *Terminate Port Diagnostics* at any time to abort the loopback test.

---

9. When the test completes, results appear as **Passed** or **Failed** in the message area of the dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port.
11. Reset the tested port:
  - a. Click the *Reset* tab. The *Port* page displays with the *Reset* tab selected.
  - b. For the tested port, click (enable) the check box in the *Port Reset* column. A check mark in the box indicates the port reset option is enabled.
  - c. Click *Activate* at the bottom of the page. The port resets and the message **Your changes have been successfully activated** appears.
12. Notify the customer the test is complete and the device can be reconnected to the director and set online.

## Performing Channel Wrap Tests (FICON)

A channel wrap test is a diagnostic procedure that checks host-to-director FICON link connectivity by returning the output of the host as input. The test is host-initiated, and transmits **ECHO** extended link service (ELS) command frames to a director port enabled for channel wrapping. The director port echoes the frames back to the host.

To perform a channel wrap test for a director-attached host:

1. Notify the customer a disruptive channel wrap test will be performed on the host-to-director FICON link.
2. At the management server, open the EFC Manager application. The *Products View* displays.
  - a. Double-click the icon representing the director for which the channel wrap test will be configured. The *Hardware View* for the selected director displays.
  - b. At the *Hardware View*, verify the location of the port to be configured for the channel wrap test. When the mouse cursor is passed over a graphical port card on the front view of the director, the card highlights with a blue border and a pop-up displays with the following information:

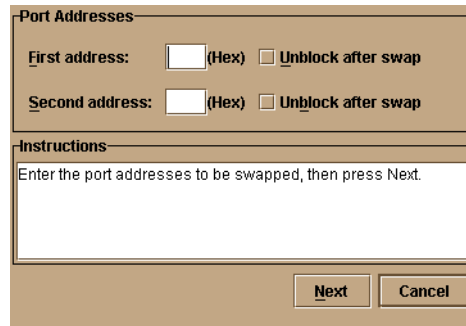
- Port card type (UPM or XPM).
  - Chassis slot number.
  - The consecutive port numbers on the selected card. Valid port numbers are in the range of **0** through **139** inclusive.
- c. Double-click the port card with the port to be configured. The *Port Card View* for the selected card displays.
  - d. Right-click the port to be configured, then select *Channel Wrap* from the menu. The *Channel Wrap On for Port n* (where *n* is the port number) window displays.
  - e. Click **OK** to enable channel wrapping for the port.
3. Perform the fibre link test at the S/390 host attached to the configured port. For test instructions, refer to the service documentation delivered with the S/390 system.

## Swapping Ports (FICON)

Use the port swap procedure to swap a device connection and logical port address from a failed Fibre Channel port to an operational port. Because both ports are blocked during the procedure, director communication with the attached device is momentarily disrupted.

To perform the port swap procedure for a pair of director ports:

1. Notify the customer a port swap procedure will be performed and a fiber-optic cable or cables will be disconnected. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. At the management server, open the EFC Manager application. The *Products View* displays.
3. Double-click the icon representing the director for which the loopback test will be performed. The *Hardware View* for the selected director displays.
4. Click *Maintenance* and select *Swap Ports*. The *Swap Ports* dialog box displays (Figure 4-18).



The dialog box is titled "Port Addresses" and "Instructions". It contains two input fields for "First address:" and "Second address:", each followed by "(Hex)" and an "Unblock after swap" checkbox. Below these is a text area for instructions. At the bottom are "Next" and "Cancel" buttons.

**Figure 4-18 Swap Ports Dialog Box**

5. At the *First address* and *Second address* fields, type the logical port addresses (in hexadecimal format) of the pair of ports to be swapped. The ports are automatically blocked during the procedure. Select the *Unblock after swap* check boxes to unblock the ports when the procedure completes.
6. Click *Next*. At the *Swap Ports* dialog box, the message **Continuing this procedure requires varying the selected ports offline. Ask the system operator to vary the link(s) offline, then press Next.** appears.
7. Click *Next*. At the *Swap Ports* dialog box, the message **Move the port cable(s). Then press Next.** appears.
8. Swap the fiber-optic jumper cables between the selected ports, then click *Next*.
9. At the *Swap Ports* dialog box, the message **Ports swapped successfully.** appears. Click *Next* to close the window and return to the *Hardware View*.

## Collecting Maintenance Data

When director operational firmware detects a critical error or FRU failure, the director automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the active CTP card, then initiates a failover to the operational FRU. The director then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the management server hard drive.

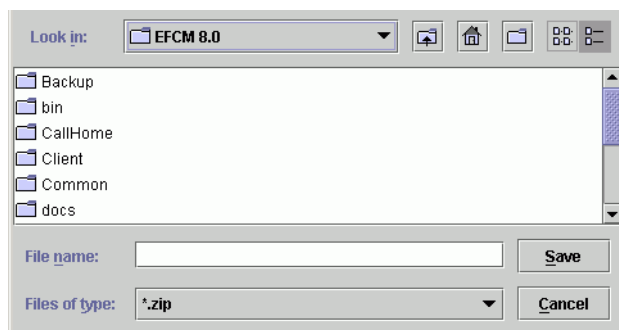
**NOTE:** An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis. Maintenance data includes the dump file, hardware log, audit log, and an engineering log viewable only by support personnel.

## Management Server

To collect maintenance data (retrieve the dump file from the management server hard drive) from the Intrepid 6140 Element Manager application:

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director for which the data collection procedure is to be performed, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Data Collection* option from the *Maintenance* menu. The *Save Data Collection* dialog box displays (Figure 4-19).

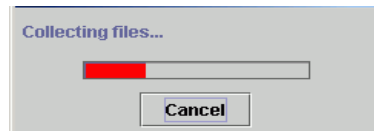


**Figure 4-19 Save Data Collection Dialog Box**

4. Remove the backup CD from the management server compact disk- rewritable (CD-RW) drive and insert a blank rewritable CD.



5. At the *Save Data Collection* dialog box, select the compact disc drive (D:\) from the *Look in* drop-down menu, then type a descriptive name for the collected maintenance data in the *File name* field.
6. The *Data Collection* dialog box (Figure 4-20) displays with a progress bar that shows percent completion of the data collection. When the process reaches 100%, the *Cancel* button changes to a *Close* Button.



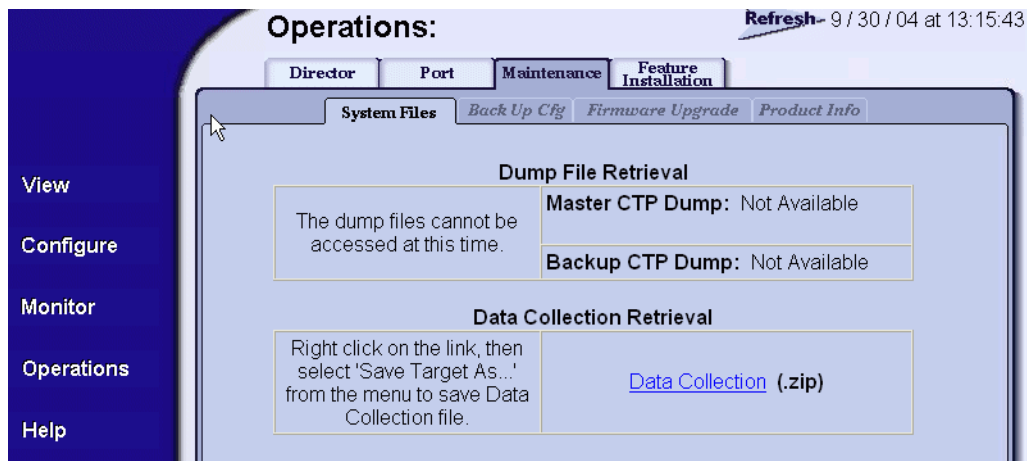
**Figure 4-20 Data Collection Dialog Box**

7. Click *Close* to close the dialog box.
8. Remove the CD with the newly-collected maintenance data from the management server CD-RW drive. Return the CD with the failed FRU to McDATA for analysis.
9. To ensure the backup application operates normally, replace the original backup CD in the management server CD-RW drive.

## SANpilot Interface

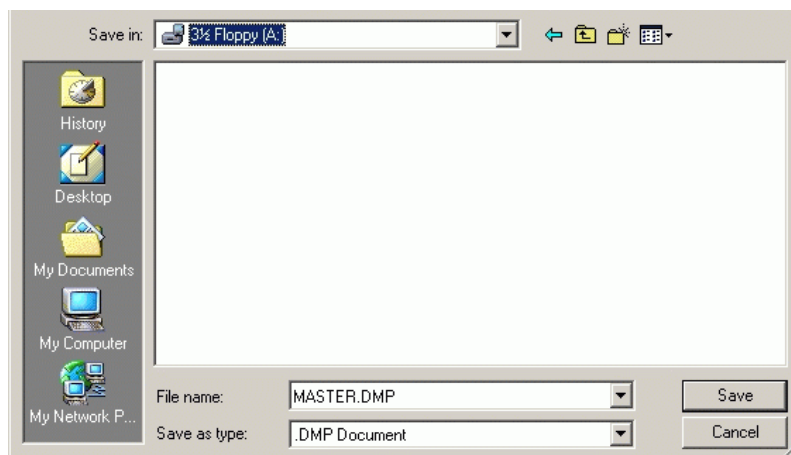
To collect maintenance data (retrieve the dump file from the CTP card) at the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Director* page displayed.
2. Click the *Maintenance* tab, then the *System Files* tab. The *Maintenance* page displays with the *System Files* tab selected (Figure 4-21).



**Figure 4-21 Operations Panel (Maintenance Page with System Files Tab)**

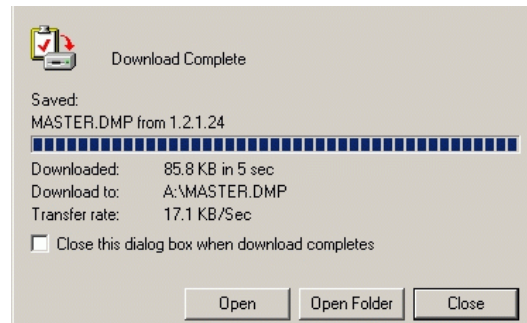
3. Right-click the *CTP Dump* link to open a list of menu options.
4. Select the *Save Target As* menu option. The *Save As* dialog box displays (Figure 4-22).



**Figure 4-22 Save As Dialog Box**

5. Insert a blank diskette in the floppy drive of the browser PC.

6. At the *Save As* dialog box, select the floppy drive (**A:\**) from the *Save in* drop-down menu, type a descriptive name for the dump file in the *File name* field, and click *Save*.
7. The *Download complete* dialog box displays (Figure 4-23) with a progress bar that shows percent completion of the dump file download.



**Figure 4-23 Download Complete Dialog Box**

8. Click *Close* to close the dialog box.
9. Remove the diskette with the newly-collected maintenance data from the browser PC floppy drive. Return the diskette with the failed FRU to McDATA for analysis.

## Set the Director Online or Offline

This section describes procedures to set the director online or offline. These operating states are described as:

- **Online** - When the director is set online, an attached device can log in to the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline** - When the director is set offline, all ports are set offline. The director transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the director.

**NOTE:** When the director is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the director offline unless directed to do so by a procedural step or the next level of support.

## Set Online State (Management Server)

To set the director online from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director to be set online, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Set Online State* option from the *Maintenance* menu. The *Set Online State* dialog box displays (Figure 4-24).

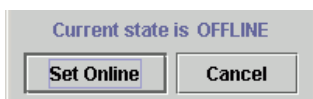


Figure 4-24 Set Online State Dialog Box

4. Click *Set Online*. A warning dialog box displays the message **Performing this operation will change the current state to Online.**
5. Click OK. As the director comes online, observe the *Hardware View*. The *Status* field of the *Intrepid 6140 Status* table displays **Online**.

## Set Offline State (Management Server)

To set the director offline from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director to be set offline, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Set Online State* option from the *Maintenance* menu. The *Set Online State* dialog box displays (Figure 4-24).
4. Click *Set Offline*. A warning dialog box displays the message **Performing this operation will change the current state to Offline.**

- Click **OK**. As the director goes offline, inspect the *Hardware View*. The *State* field of the *Intrepid 6140 Status* table displays **Offline**.

## Set Online State (SANpilot Interface)

To set the director online from the SANpilot interface:

- When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
- Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected (Figure 4-25).
- Click **Set Online**. The director comes online and the message **Your changes have been successfully activated** appears.

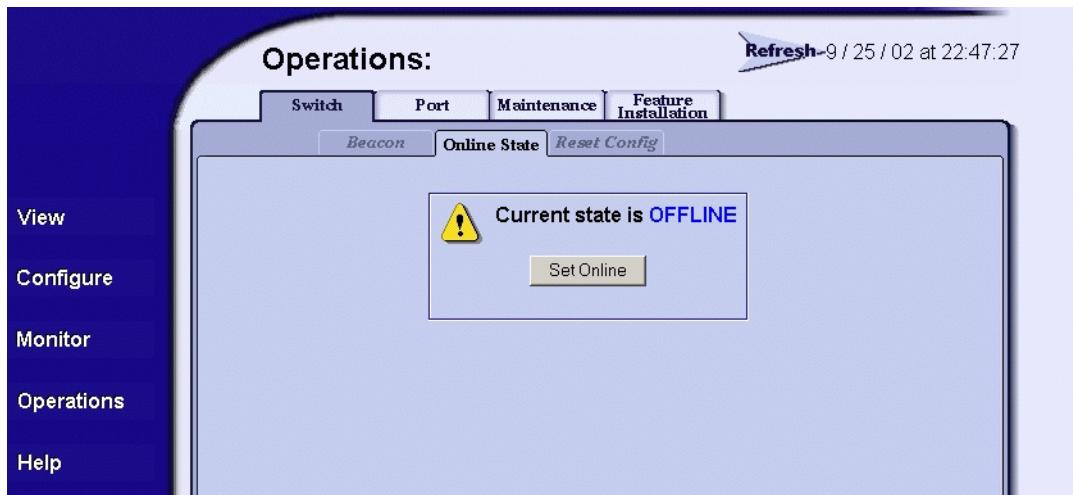


Figure 4-25 Operations Panel (Switch Page with Online State Tab)

## Set Offline State (SANpilot Interface)

To set the director offline from the SANpilot interface:

- When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
- Click the *Online State* tab. The *Switch* page displays with the *Online State* tab selected (Figure 4-25).

3. Click Set Offline. The director goes offline and the message **Your changes have been successfully activated** appears.

## Blocking and Unblocking Ports

This section describes procedures to block or unblock director ports. An entire port card can be blocked or unblocked, or ports can be blocked or unblocked on an individual basis. When a port is blocked, the port is automatically set offline. When a port is unblocked, the port is automatically set online.

**NOTE:** When a director port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block director ports unless directed to do so by a procedural step or the next level of support.

### Block a Port (Management Server)

To block a director port from the management server (Intrepid 6140 Element Manager application):

1. Notify the customer the port will be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. At the management server, open the SAN management application (SANavigator or EFCM).
3. At the SAN management application physical map, right-click the product icon representing the director for which the port is to be blocked, then select *Element Manager* from the pop-up menu. The application opens.
4. Click the *Hardware* tab. The *Hardware View* for the selected director displays.
5. Move the cursor over the port to be blocked and right-click the mouse to open a list of menu options.
6. Select the *Block Port* menu option. A *Warning* dialog box displays (Figure 4-26).

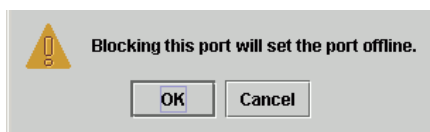


Figure 4-26 Blocking Port Warning Box

7. Click *OK*. The following occur to indicate the port is blocked and offline:
  - The emulated green LED associated with the port extinguishes at the *Hardware View*.
  - The green LED associated with the port extinguishes at the director.
  - A check mark displays in the check box adjacent to the *Block Port* menu option.

---

### Block a Port Card (Management Server)

To block all ports on a director port card from the management server (Intrepid 6140 Element Manager application):

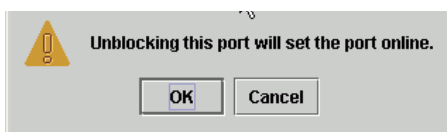
1. Notify the customer the port card will be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. At the management server, open the SAN management application (SANavigator or EFCM).
3. At the SAN management application physical map, right-click the product icon representing the director for which the port is to be blocked, then select *Element Manager* from the pop-up menu. The application opens.
4. Click the *Hardware* tab. The *Hardware View* for the selected director displays.
5. Move the cursor over the port card to be blocked and right-click the mouse to open a list of menu options.
6. Select the *Block All Ports* menu option. A *Warning* dialog box displays
7. Click *OK*. The following occur to indicate the port card is blocked and offline:
  - Emulated green LEDs associated with all ports extinguish at the *Hardware View*.
  - Green LEDs associated with all ports extinguish at the director.

---

### Unblock a Port (Management Server)

To unblock a director port from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director for which the port is to be unblocked, then select *Element Manager* from the pop-up menu. The application opens.
3. Click the *Hardware* tab. The *Hardware View* for the selected director displays.
4. Move the cursor over the port to be unblocked and right-click the mouse to open a list of menu options.
1. Select the *Block Port* menu option. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. A *Warning* dialog box displays (Figure 4-27).



**Figure 4-27 Unblocking Port Warning Box**

2. Click OK. The following occur to indicate the port is unblocked and online:
  - The emulated green LED associated with the port illuminates at the *Hardware View*.
  - The green LED associated with the port illuminates at the director.
  - The check box adjacent to the *Block Port* menu option becomes blank.

### Unblock a Port Card (Management Server)

To unblock all ports on a director port card from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director for which the port is to be unblocked, then select *Element Manager* from the pop-up menu. The application opens.



3. Click the *Hardware* tab. The *Hardware View* for the selected director displays.
4. Move the cursor over the port card to be unblocked and right-click the mouse to open a list of menu options.
5. Select the *Unblock All Ports* menu option. A *Warning* dialog box displays.
6. Click *OK*. The following occur to indicate the port card is unblocked and online:
  - Emulated green LEDs associated with all ports illuminate at the *Hardware View*.
  - Green LEDs associated with all ports illuminate at the director.

### Block a Port (SANpilot Interface)

To block a director port from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-28).

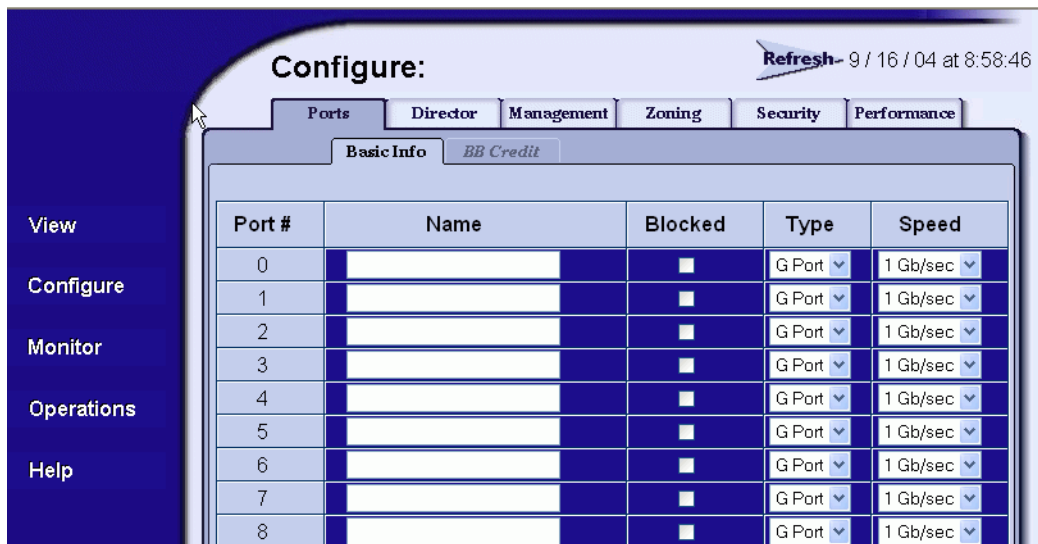


Figure 4-28 Configure Panel (Ports Page)

2. Click the check box for the selected port in the *Blocked* column to block the port (default is unblocked). A check mark in the box indicates the port is blocked.
3. Click *Activate* at the bottom of the page to save and activate the blocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

---

### Unblock a Port (SANpilot Interface)

To unblock a director port from the SANpilot interface:

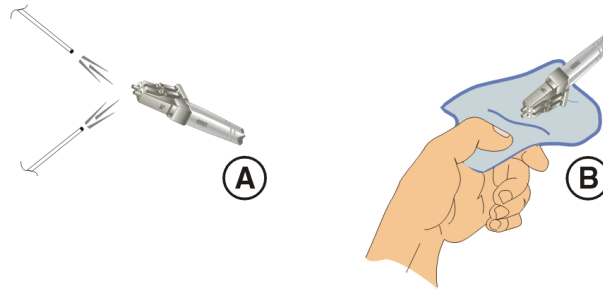
1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Configure* option at the left side of the panel. The *Configure* panel opens with the *Ports* page displayed (Figure 4-28).
2. Click the check box for the selected port in the *Blocked* column to remove the check mark and unblock the port. A blank box indicates the port is unblocked.
3. Click *Activate* at the bottom of the page to save and activate the unblocked configuration. The message **Your changes to the port configuration have been successfully activated** appears.

---

## Cleaning Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port card connectors (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the port. Use compressed air to blow any contaminants from the connector (part **A** of Figure 4-29).
  - Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
  - Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.



**Figure 4-29 Clean Fiber-Optic Components**

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad (part **B** of [Figure 4-29](#)). Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
4. Repeat [step 2](#) and [step 3](#) of this procedure (second cleaning).
5. Repeat [step 2](#) and [step 3](#) of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

## Power-On Procedure



### **DANGER**

*Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.*

To power on the director:

1. One alternating current (AC) power cord is required for each power supply installed. Ensure power cord(s) connect facility power to the input AC module at the bottom rear of the director.

**NOTE:** If two power cords are installed for high availability, plug the cords into separate facility power circuits.

**NOTE:** The director does not have a power switch. Therefore the director powers on when its power cords are connected to facility power.

2. The director powers on and performs power-on self-tests (POSTs). During POSTs:
  - Amber LEDs on both CTP cards and all port cards illuminate momentarily.
  - Green LED on each CTP card (active and backup) and each port card illuminate as the card is tested.
  - Green LEDs associated with Fibre Channel ports sequentially illuminate as the ports are tested.
3. After successful POST completion, the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated.
4. If a POST error or other malfunction occurs, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

---

**NOTE:** When powering on the director after removing and replacing a faulty FRU, the amber system error LED may remain illuminated. Clear the system error LED as part of the replacement procedure.

---

## Power-Off Procedure

Powering the director off and on (performing a power cycle) resets all logic cards and executes POSTs. When performing a power cycle, wait approximately 30 seconds before switching power on.

---

**NOTE:** When the director is powered off, the operation of attached Fibre Channel devices is disrupted. Do not power off the director unless directed to do so by a procedural step or the next level of support.

---

To power off the director:

1. Notify the customer the director will be powered off. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set the Director Online or Offline](#) on page 4-43).
3. Remove the director power cords from facility power. The director powers off.

4. If servicing the director, disconnect power cord(s) from the input AC module at the bottom rear of the director. This step is not required when performing a power cycle.

---

## IML, IPL, or Reset the Director

This section describes procedures to IML, IPL, or reset the Intrepid 6140 Director. An IML or reset is performed at the CTP front panel using the **IML** or the **RESET** button. An IPL is performed from the management server (Intrepid 6140 Element Manager application). The SANpilot interface does not provide an IML, IPL, or director reset function.

---

**ATTENTION!** A reset should only be performed if a CTP card failure is indicated. Do not reset the director unless directed to do so by a procedural step or the next level of support.

---

An IML and IPL are functionally equivalent. The operations do not cause power-on diagnostics to execute and are not disruptive to Fibre Channel traffic. Both operations:

- Reload director firmware from FLASH memory.
- Reset the Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.

A director reset is more disruptive and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during director reset must be retransmitted.

---

### IML the Director (CTP Front Panel)

To IML the director from the CTP front panel:

1. Press and hold the **IML** button for approximately three seconds.

2. During the IML, the director-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
  - As the network connection drops, the *Intrepid 6140 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
  - The status bar at the bottom of the window displays a grey square, indicating director status is unknown.
  - Illustrated FRUs disappear, and appear again as the connection is re-established.

### IPL the Director (Management Server)

To IPL the director from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director requiring an IPL, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *IPL* option from the *Maintenance* menu. An *Information* dialog box displays (Figure 4-30).

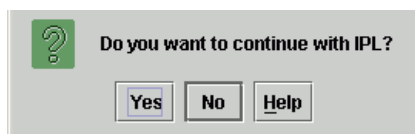


Figure 4-30 Information Dialog Box

4. Click *Yes* to IPL the director. During the IPL, the director-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
  - As the network connection drops, the *Intrepid 6140 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
  - The status bar at the bottom of the window displays a grey square, indicating director status is unknown.
  - Illustrated FRUs disappear, and appear again as the connection is re-established.

---

## Reset the Director (CTP Front Panel)

To reset the director from the CTP front panel:

1. Press and hold the **RESET** button for approximately three seconds.
2. During the reset:
  - The green power (**PWR**) LED on the director front panel illuminates.
  - The amber system error (**ERR**) LED on the director front panel blinks momentarily while the director is tested.
  - The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
  - The amber LEDs associated with the ports blink momentarily while the ports are tested.
  - The director-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
    - As the network connection drops, the *Intrepid 6140 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
    - The status bar at the bottom of the window displays a grey square, indicating director status is unknown.
    - Illustrated FRUs disappear, and appear again as the connection is re-established.

---

## Managing Firmware Versions

Firmware is the director operating code stored in FLASH memory on the CTP card. Up to 32 firmware versions can be stored on the management server hard drive and made available for download to a director through the Intrepid 6140 Element Manager application. Multiple firmware versions can be stored on a browser PC hard drive and made available for download to the director from the SANpilot interface.

---

## Management Server

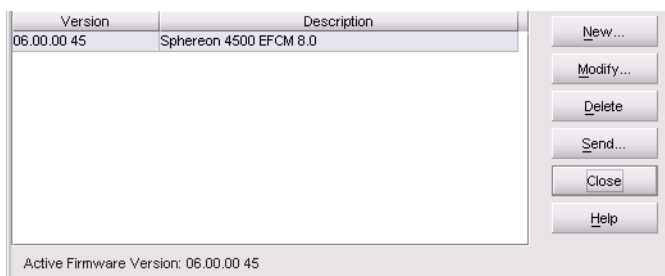
Service personnel can perform the following firmware management tasks from the management server (Intrepid 6140 Element Manager application):

- Determine the firmware version active on a director.
- Add to and maintain a library of up to 32 firmware versions on the management server hard drive.
- Download a firmware version to a selected director.

### Determine a Director Firmware Version

To determine a selected director firmware version from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director to be inspected for firmware version, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays (Figure 4-31).



**Figure 4-31 Firmware Library Dialog Box**

4. The firmware version displays at the lower left corner of the dialog box in *XX.YY.ZZ* format, where *XX* is the version level, *YY* is the release level, and *ZZ* is the patch level.
5. Click *Close* to close the dialog box.

### Add a Firmware Version to the Management Server Library

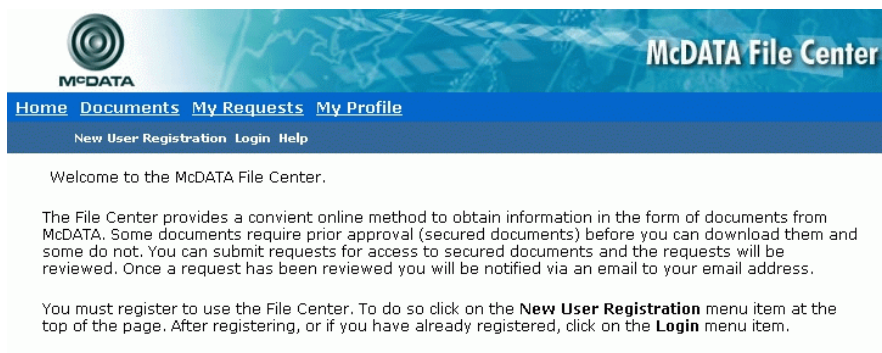
The firmware version shipped with the director is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent firmware versions for upgrading the director are provided to customers through the McDATA Internet home page.



**NOTE:** When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the code. This information supplements information provided in this general procedure.

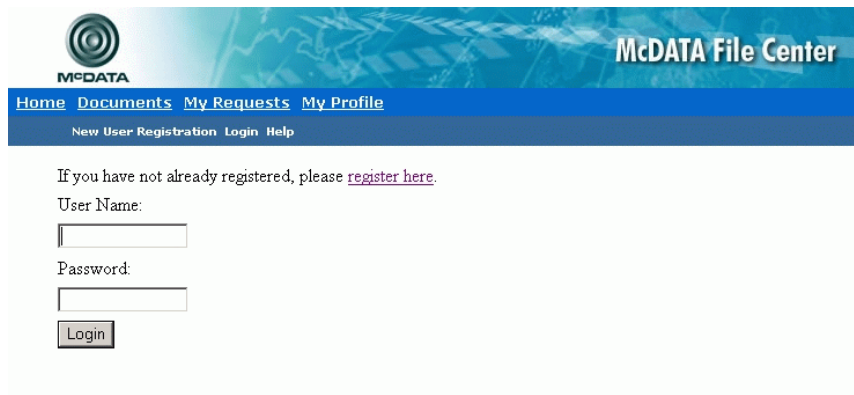
To add a director firmware version to the library stored on the management server hard drive:

1. Obtain the new firmware version from the McDATA File Center. At a PC with Internet access, open the File Center home page (Figure 4-32). The uniform resource locator (URL) is <http://central.mcddata.com>.



**Figure 4-32** McDATA File Center Home Page

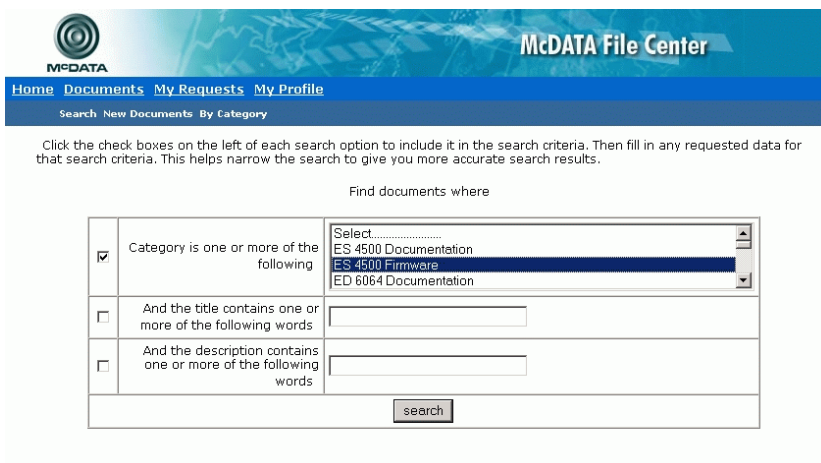
2. Select (click) the *Login* option at the top of the home page. The *Login* page displays (Figure 4-33).



The screenshot shows the McDATA File Center login page. At the top is the McDATA logo and the text 'McDATA File Center'. Below this is a navigation bar with links: Home, Documents, My Requests, My Profile. Underneath the navigation bar are links for New User Registration, Login, and Help. The main content area contains a message: 'If you have not already registered, please [register here](#).' Below this are input fields for 'User Name:' and 'Password:', followed by a 'Login' button.

**Figure 4-33 McDATA File Center (Login Page)**

3. Type the user name and password (assigned and registered while performing *Task 15: Register with the McDATA File Center* on page 2-120) and click *Login*. The *Welcome* page displays.
4. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays (Figure 4-34).



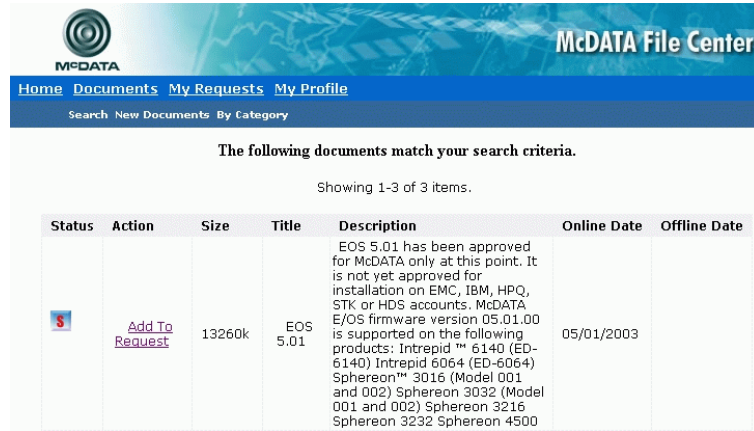
The screenshot shows the McDATA File Center 'Find Documents' page. It features the same header and navigation bar as Figure 4-33. Below the navigation bar, there is a search section with the text: 'Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.' The search options are listed in a table-like structure:

Find documents where	
<input checked="" type="checkbox"/>	Category is one or more of the following
<input type="checkbox"/>	And the title contains one or more of the following words
<input type="checkbox"/>	And the description contains one or more of the following words

Below the table is a search button labeled 'search'.

**Figure 4-34 McDATA File Center (Find Documents Page)**

5. Select (highlight) the *ED 6140 Firmware* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-35) with a list of firmware available for download.



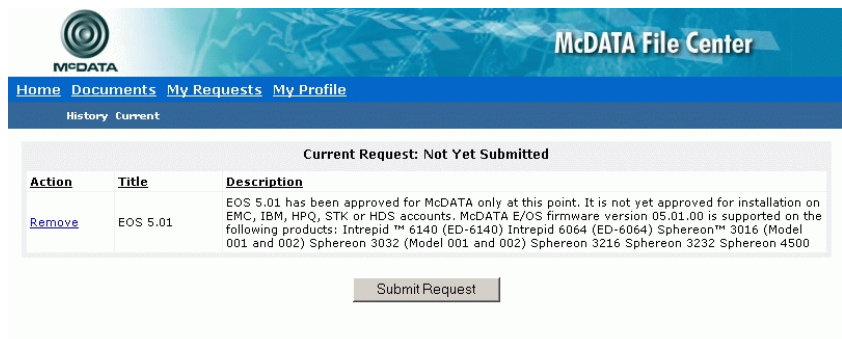
The following documents match your search criteria.

Showing 1-3 of 3 items.

Status	Action	Size	Title	Description	Online Date	Offline Date
	<a href="#">Add To Request</a>	13260k	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Spheron™ 3016 (Model 001 and 002) Spheron 3032 (Model 001 and 002) Spheron 3216 Spheron 3232 Spheron 4500	05/01/2003	

Figure 4-35 McDATA File Center (Documents Match Page)

6. Authorization to download a firmware version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired firmware version, click *Add to Request*. The *Current Request* page displays (Figure 4-36).



Current Request: Not Yet Submitted

Action	Title	Description
<a href="#">Remove</a>	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Spheron™ 3016 (Model 001 and 002) Spheron 3032 (Model 001 and 002) Spheron 3216 Spheron 3232 Spheron 4500

[Submit Request](#)

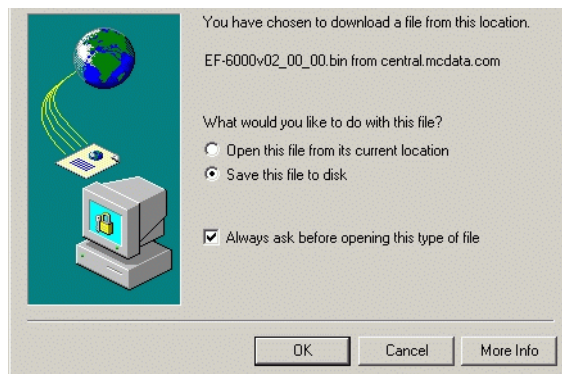
Figure 4-36 McDATA File Center (Current Request Page)

7. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-37) with the approved request.



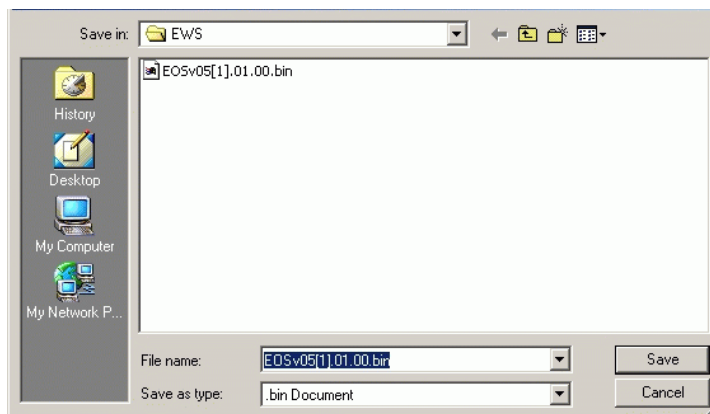
**Figure 4-37 McDATA File Center (Request History Page)**

8. In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays (Figure 4-38).



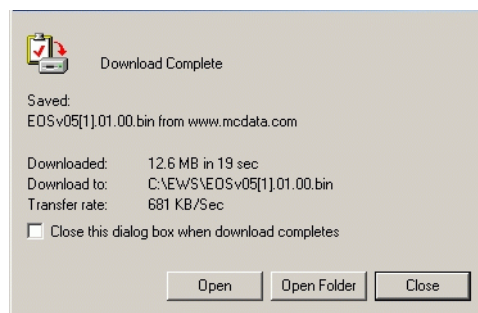
**Figure 4-38 File Download Dialog Box**

9. Select the *Save this file to disk* radio button and click *OK*. The *Save As* dialog box appears (Figure 4-39).



**Figure 4-39 Save As Dialog Box**

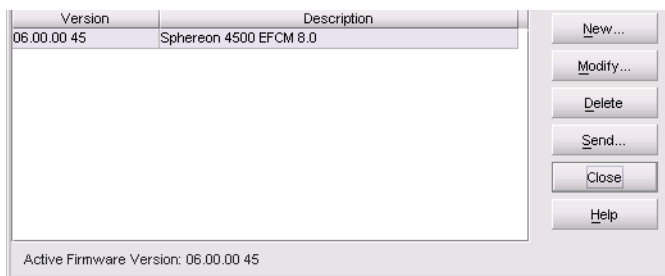
10. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field and the correct file is specified in the *File name* field. Click *Save*.
11. The *Download complete* dialog box displays (Figure 4-40) with a progress bar that shows percent completion of the firmware version download.
12. When the process completes, click *Close* to close the dialog box. The new firmware version is downloaded and saved to the PC hard drive.



**Figure 4-40 Download Complete Dialog Box**

13. At the PC, close the Internet session.
14. Transfer the firmware version file from the PC to the management server by diskette, CD-ROM, or other electronic means.

15. At the management server, open the SAN management application (SANavigator or EFCM).
16. At the SAN management application physical map, right-click the product icon representing the director for which a firmware version is to be added, then select *Element Manager* from the pop-up menu. The application opens.
17. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays (Figure 4-41).



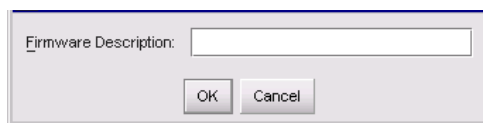
**Figure 4-41 Firmware Library Dialog Box**

18. Click *New*. The *New Firmware Version* dialog box displays (Figure 4-42).



**Figure 4-42 New Firmware Version Dialog Box**

19. Select the desired firmware version file (downloaded in [step 1](#)) from the management server diskette drive or hard drive. Ensure the correct directory path and filename appear in the *File name* field and click *Save*. The *New Firmware Description* dialog box displays (Figure 4-43).



**Figure 4-43 New Firmware Description Dialog Box**

20. Enter a description (up to 24 characters) for the new firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.
21. A *Transfer Complete* message box displays (Figure 4-44). As the transfer progresses, a progress bar travels across the message box to show percent completion.



**Figure 4-44 File Transfer Message Box**

22. The *File Transfer* message box converts to a *Transfer Complete* message box, indicating the new firmware version is stored on the management server hard drive. Click *Close* to close the message box.
23. The new firmware version and associated description appear in the *Firmware Library* dialog box. Click *Close* to close the window and return to the *Hardware View*.
24. To send the firmware version to a director, see [Download a Firmware Version to a Director](#) following.

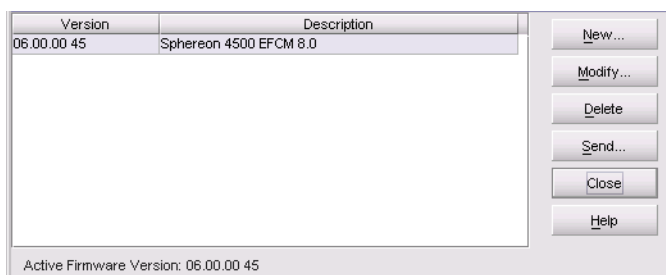
### Download a Firmware Version to a Director

**NOTE:** When downloading a firmware version, follow procedural information in release notes or EC instructions that accompany the firmware version. This information supplements information provided in this general procedure.

To download a firmware version to a selected director from the management server (Intrepid 6140 Element Manager application):

1. At the management server, open the SAN management application (SANavigator or EFCM).

2. Before downloading firmware version **XX.YY.ZZ** to a director, ensure version **XX.YY.ZZ** or higher of the SAN management application is running on the server.
  - a. Select the *About* option from the *Help* menu. The *About* dialog box displays the SAN management application version. Click *Close* to close the dialog box.
  - b. If required, install the correct version of the application ([Installing or Upgrading Software](#) on page 4-82).
3. At the SAN management application physical map, right-click the product icon representing the director for which a firmware version is to be downloaded, then select *Element Manager* from the pop-up menu. The application opens.
4. As a precaution to preserve director configuration information, perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
5. Select the *Firmware Library* option from the *Maintenance* menu. The *Firmware Library* dialog box displays ([Figure 4-45](#)).

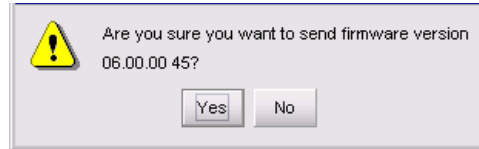


**Figure 4-45 Firmware Library Dialog Box**

6. Select (highlight) the firmware version to be downloaded and click *Send*. The send function verifies existence of certain director conditions before the download begins. If an error occurs, a message displays indicating the problem must be fixed before firmware is downloaded. Conditions that terminate the process include:
  - A redundant CTP card failure.
  - The firmware version is being installed to the director by another user.
  - The director-to-management server link is down.



If a problem occurs and a corresponding message displays, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem. If no error occurs, a *Warning* dialog box displays ([Figure 4-46](#)).



**Figure 4-46 Warning Dialog Box**

7. Click *Yes* to download the firmware version. The *Send Firmware* dialog box displays ([Figure 4-47](#)) and the following occur during the download:
  - a. As the download begins, a **Writing data to FLASH** message displays at the top of the dialog box for a few moments.
  - b. As the download progresses, a **Sending Files** message displays. This message remains as a progress bar travels across the dialog box to show percent completion of the download. The bar progresses to 100% when the last file is transmitted to the CTP card.
  - c. As the download finishes, a **Writing data to FLASH** message displays again for a few moments.
  - d. The director performs an IPL, during which an **IPLing** message displays at the *Send Firmware* dialog box. In addition, the director-to-management server Ethernet link drops momentarily and the following occur at the *Hardware View*:
    - As the network connection drops, the *Intrepid 6140 Status* table turns yellow, the *Status* field displays **No Link**, and the *State* field displays **Link Timeout**.
    - The status bar at the bottom of the window displays a grey square, indicating director status is unknown.
    - Illustrated FRUs disappear, and appear again as the connection is re-established.
8. After the IPL, a **Send firmware complete** message displays at the *Send Firmware* dialog box ([Figure 4-47](#)). Click *Close*.
9. Click *Close* to close the *Firmware Library* dialog box.

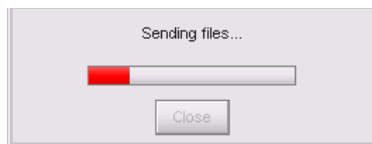


Figure 4-47 Send Firmware Dialog Box

## SANpilot Interface

Service personnel can perform the following firmware management tasks from the SANpilot interface:

- Determine the firmware version actively running on the director.
- Add a firmware versions to the browser PC hard drive.
- Download a firmware version to the director.

### Determine Director Firmware Version

To determine a director firmware version from the SANpilot interface:

1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, click the *Unit Properties* tab. The *Unit Properties* page displays (Figure 4-48).
2. At the bottom of the page, record the firmware version listed in the *Firmware Level* field.

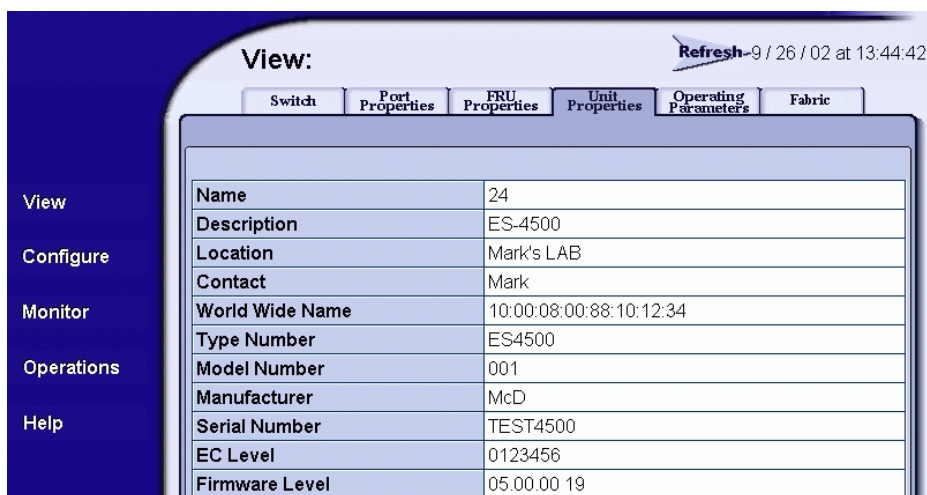


Figure 4-48 View Panel (Unit Properties Page)

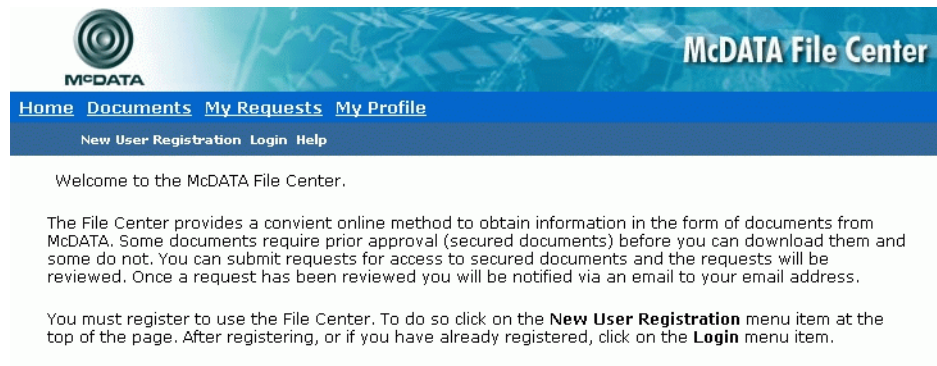
## Add a Firmware Version to the Browser PC Hard Drive

The firmware version shipped with the director is provided on the *System Version XX.YY.ZZ* CD-ROM. Subsequent firmware versions for upgrading the director are provided to customers through McDATA website.

**NOTE:** When adding a firmware version, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the code. This information supplements information provided in this general procedure.

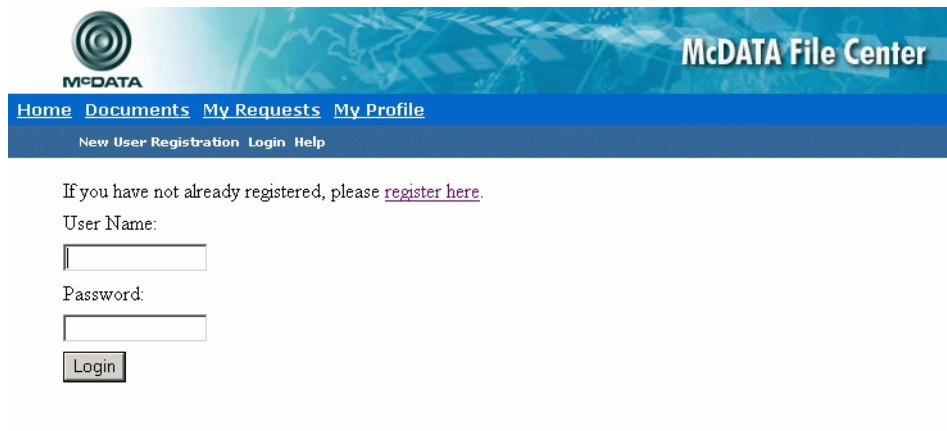
To add a director firmware version to the browser PC hard drive (PC running the SANpilot interface):

1. Obtain the new firmware version from the McDATA File Center. At a PC with Internet access, open the File Center home page ([Figure 4-49](#)). The uniform resource locator (URL) is <http://central.mcddata.com>.



**Figure 4-49 McDATA File Center Home Page**

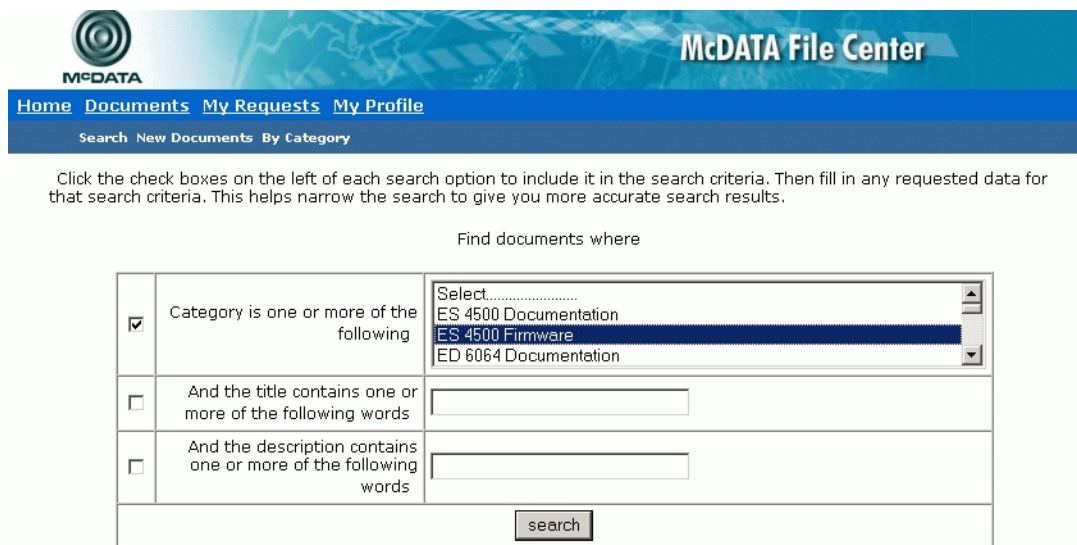
2. Select (click) the *Login* option at the top of the home page. The *Login* page displays ([Figure 4-50](#)).



The image shows the login page of the McDATA File Center. At the top, there is a blue header with the McDATA logo on the left and the text "McDATA File Center" on the right. Below the header is a navigation bar with links: "Home", "Documents", "My Requests", and "My Profile". Underneath this is another bar with "New User Registration", "Login", and "Help". The main content area has a light blue background. It starts with a message: "If you have not already registered, please [register here](#)." Below this are two input fields: "User Name:" and "Password:". At the bottom of these fields is a "Login" button.

**Figure 4-50 McDATA File Center (Login Page)**

3. Type the user name and password (assigned and registered while performing *Task 15: Register with the McDATA File Center* on page 2-120) and click *Login*. The *Welcome* page displays.
4. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays (Figure 4-51).



The image shows the "Find Documents" page of the McDATA File Center. It has the same header and navigation bar as Figure 4-50. Below the navigation bar, there is a section titled "Find documents where". It contains three search criteria, each with a checkbox and a text input field:
 

- Category is one or more of the following: This criterion is selected (checkbox checked). The dropdown menu shows "Select.....", "ES 4500 Documentation", "ES 4500 Firmware" (highlighted), and "ED 6064 Documentation".
- And the title contains one or more of the following words: This criterion is not selected (checkbox unchecked). The text input field is empty.
- And the description contains one or more of the following words: This criterion is not selected (checkbox unchecked). The text input field is empty.

 At the bottom of the search criteria section is a "search" button.

**Figure 4-51 McDATA File Center (Find Documents Page)**

5. Select (highlight) the *ED 6140 Firmware* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-52) with a list of firmware available for download.



**McDATA File Center**

Home Documents My Requests My Profile

Search New Documents By Category

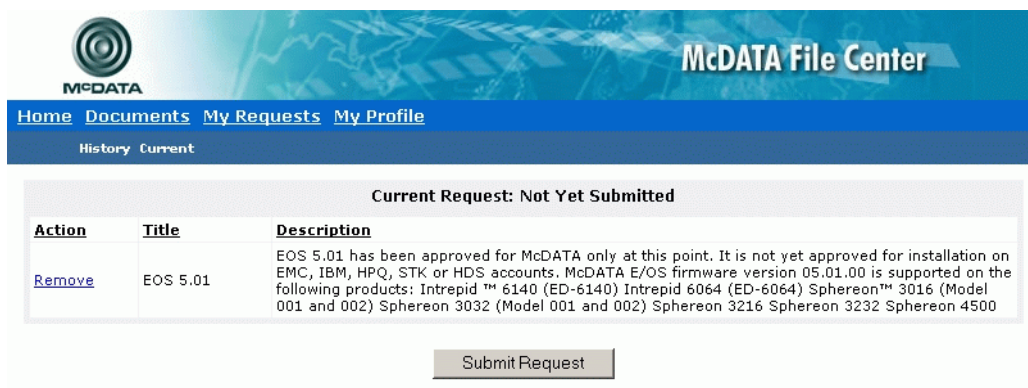
The following documents match your search criteria.

Showing 1-3 of 3 items.

Status	Action	Size	Title	Description	Online Date	Offline Date
	<a href="#">Add To Request</a>	13260k	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500	05/01/2003	

Figure 4-52 McDATA File Center (Documents Match Page)

6. Authorization to download a firmware version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired firmware version, click *Add to Request*. The *Current Request* page displays (Figure 4-53).



**McDATA File Center**

Home Documents My Requests My Profile

History Current

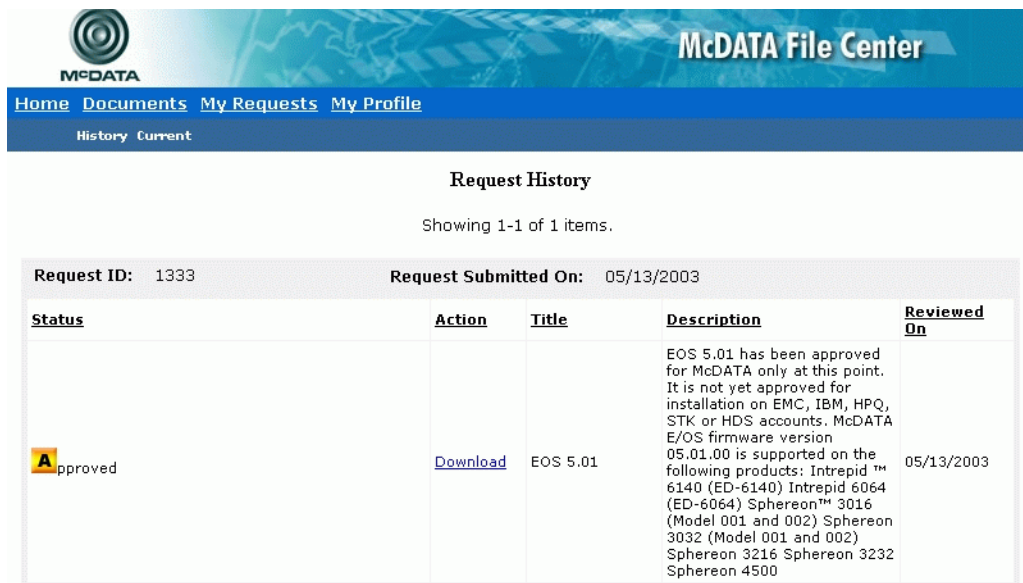
Current Request: Not Yet Submitted

Action	Title	Description
<a href="#">Remove</a>	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500

[Submit Request](#)

Figure 4-53 McDATA File Center (Current Request Page)

7. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-54) with the approved request.



**McDATA File Center**


Home Documents My Requests My Profile

History Current

**Request History**

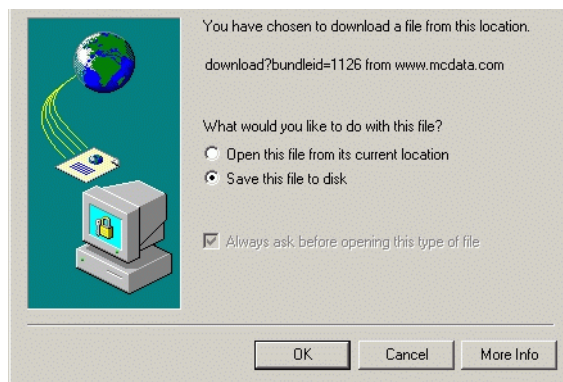
Showing 1-1 of 1 items.

Request ID: 1333 Request Submitted On: 05/13/2003

Status	Action	Title	Description	Reviewed On
 Approved	<a href="#">Download</a>	EOS 5.01	EOS 5.01 has been approved for McDATA only at this point. It is not yet approved for installation on EMC, IBM, HPQ, STK or HDS accounts. McDATA E/OS firmware version 05.01.00 is supported on the following products: Intrepid™ 6140 (ED-6140) Intrepid 6064 (ED-6064) Sphereon™ 3016 (Model 001 and 002) Sphereon 3032 (Model 001 and 002) Sphereon 3216 Sphereon 3232 Sphereon 4500	05/13/2003

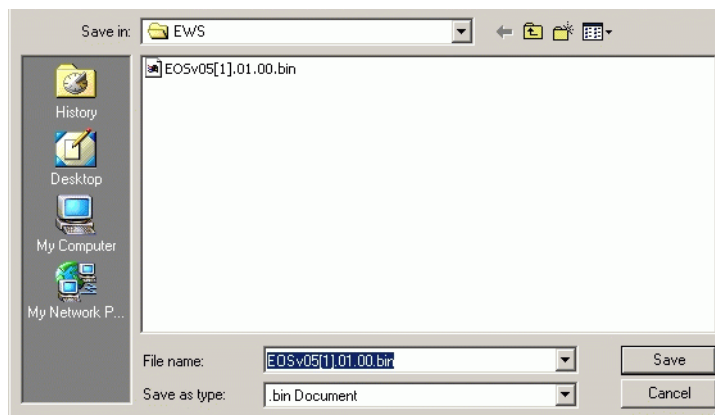
**Figure 4-54 McDATA File Center (Request History Page)**

8. In the *Action* column adjacent to the approved request for the firmware version, click *Download*. The *File Download* dialog box displays (Figure 4-55).



**Figure 4-55 File Download Dialog Box**

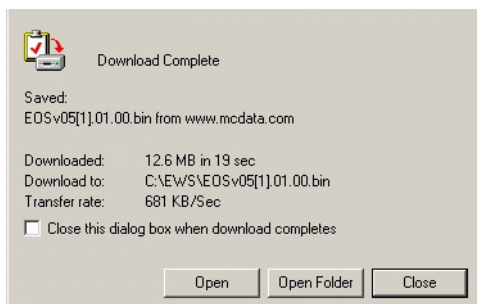
9. Select the *Save this file to disk* radio button and click OK. The *Save As* dialog box appears (Figure 4-56).



**Figure 4-56 Save As Dialog Box**

10. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field, the correct file is specified in the *File name* field, and click *Save*.
11. A *Download* dialog box displays, showing the estimated time remaining to complete the download. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-57).





**Figure 4-57 Download Complete Dialog Box**

12. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the browser PC hard drive.
13. At the browser PC, close the Internet session.

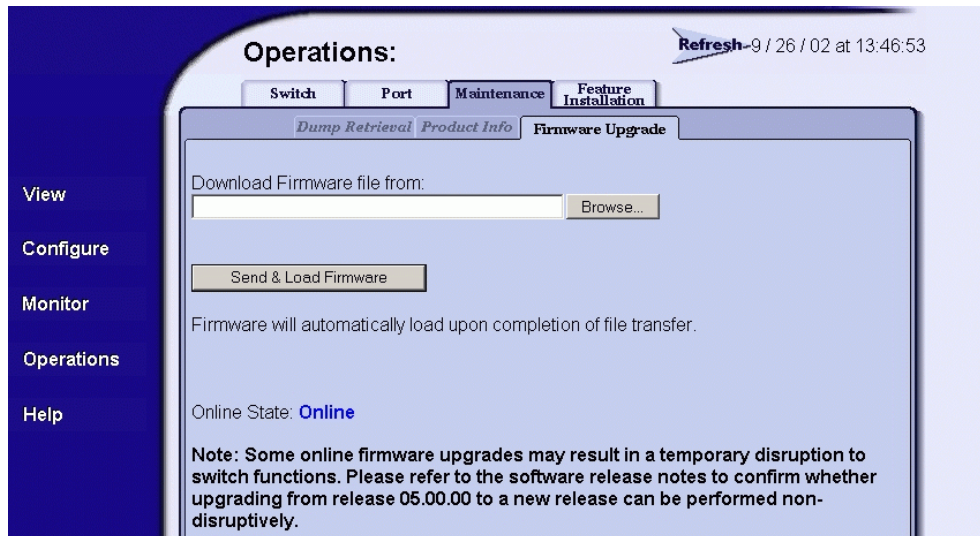
### Download a Firmware Version to the Director

To download a firmware version to the director from the SANpilot interface:

**NOTE:** When downloading a firmware version, follow all procedural information contained in release notes or EC instructions that accompany the firmware version. This information supplements information provided in this general procedure.

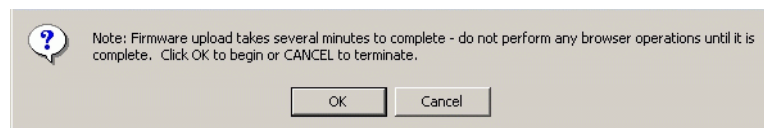
1. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
2. Click the *Maintenance* and *Firmware Upgrade* tabs. The *Maintenance* page displays with the *Firmware Upgrade* tab selected (Figure 4-58).





**Figure 4-58 Operations Panel (Maintenance Page with Firmware Upgrade Tab)**

3. At the *Download Firmware file from* field:
  - Select the desired firmware file from the PC hard drive using the *Browse* button, or
  - Type the desired firmware filename in the *Download Firmware file from* field.
4. Click *Send and Load Firmware*. A browser-specific message box displays (Figure 4-59).



**Figure 4-59 Browser-Specific Message Box**

5. Click *OK* to download the firmware version to the director. The download takes several minutes to complete, during which the browser is unavailable.
6. When the firmware version is downloaded to the director and verified, this message box displays (Figure 4-60).

**Firmware successfully received and verified.  
Your browser connection will be unavailable  
until unit restart is complete.**

If your browser is not redirected to the Firmware Complete Acknowledgement page within 30 seconds, click [here](#).

**Figure 4-60 Firmware Received Message Box**

7. After firmware verification, the director performs an IPL that takes approximately 30 seconds to complete. During the IPL, the browser-to-director Internet connection drops momentarily and the SANpilot session is lost.
8. After the director IPL and SANpilot session logout, this message box displays ([Figure 4-61](#)).



**Figure 4-61 Firmware Upgrade Complete Message Box**

9. Click [here](#) to login to the director and start a new SANpilot session. The *Enter Network Password* dialog box displays.
10. Type the default user name and password.

**NOTE:** The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

11. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed.

## Managing Configuration Data

The Intrepid 6140 Element Manager application provides options to back up and restore the configuration files stored in nonvolatile random-access memory (NV-RAM) on both director CTP cards. The SANpilot interface and the Intrepid 6140 Element Manager application both provide the option to reset the configuration file to factory default values.

---

**NOTE:** The director must be set offline prior to restoring the configuration file.

---

Configuration data in the file includes:

- Director identification data.
- Port configuration data.
- Director and fabric operating parameters.
- Simple network management protocol (SNMP) configuration information.
- Zoning configuration information.

---

**NOTE:** The Element Manager application and the SANpilot interface provide the option to reset the configuration file to factory defaults. The director must be set offline prior to resetting the configuration file.

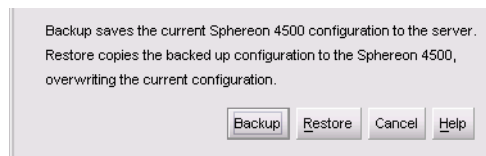
---

---

## Back Up the Configuration

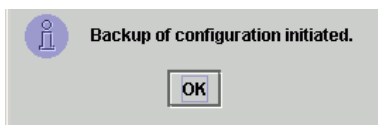
To back up the director configuration file to the management server using the Intrepid 6140 Element Manager application:

1. At the management server, open the SAN management application (SANavigator or EFCM).
2. At the SAN management application physical map, right-click the product icon representing the director for which a configuration file is to be backed up, then select *Element Manager* from the pop-up menu. The application opens.
3. Select the *Backup & Restore Configuration* option from the *Maintenance* menu. The *Backup and Restore Configuration* dialog box displays (Figure 4-62).



**Figure 4-62 Backup and Restore Configuration Dialog Box**

4. Click *Backup*. An *Information* dialog box displays, indicating the backup operation was initiated (Figure 4-63).



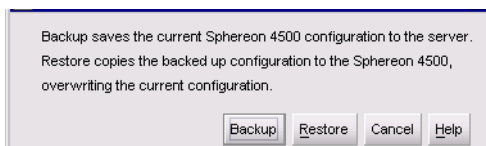
**Figure 4-63 Information Dialog Box**

5. Click *OK* to complete the backup and close the dialog box.

## Restore the Configuration

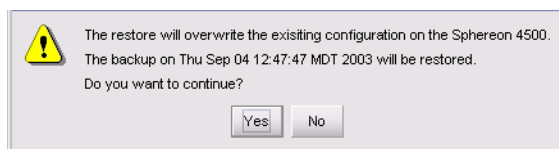
To restore the director configuration file from the management server using the Intrepid 6140 Element Manager application:

1. Notify the customer the director will be set offline. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline ([Set the Director Online or Offline](#) on page 4-43).
3. At the management server, open the SAN management application (SANavigator or EFCM).
4. At the SAN management application physical map, right-click the product icon representing the director for which a configuration file is to be restored, then select *Element Manager* from the pop-up menu. The application opens.
5. Select the *Backup & Restore Configuration* option from the *Maintenance* menu. The *Backup and Restore Configuration* dialog box displays (Figure 4-64).



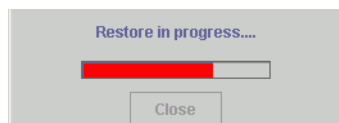
**Figure 4-64 Backup and Restore Configuration Dialog Box**

6. Click *Restore*. A *Warning* dialog box displays, indicating the existing configuration file is to be overwritten (Figure 4-65).



**Figure 4-65 Warning Dialog Box**

7. Click *Yes*. A *Restore* dialog box displays, indicating the restore operation is in progress ([Figure 4-66](#)).
8. When the operation finishes, the *Restore* dialog box displays a **Restore complete** message. Click *Close* to close the dialog box.



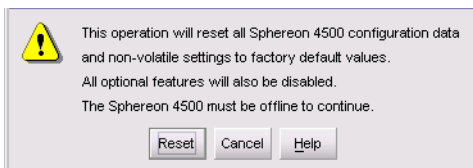
**Figure 4-66 Restore Dialog Box**

## Reset Configuration Data (Management Server)

**NOTE:** When director configuration data is reset to factory default values, all optional features are disabled.

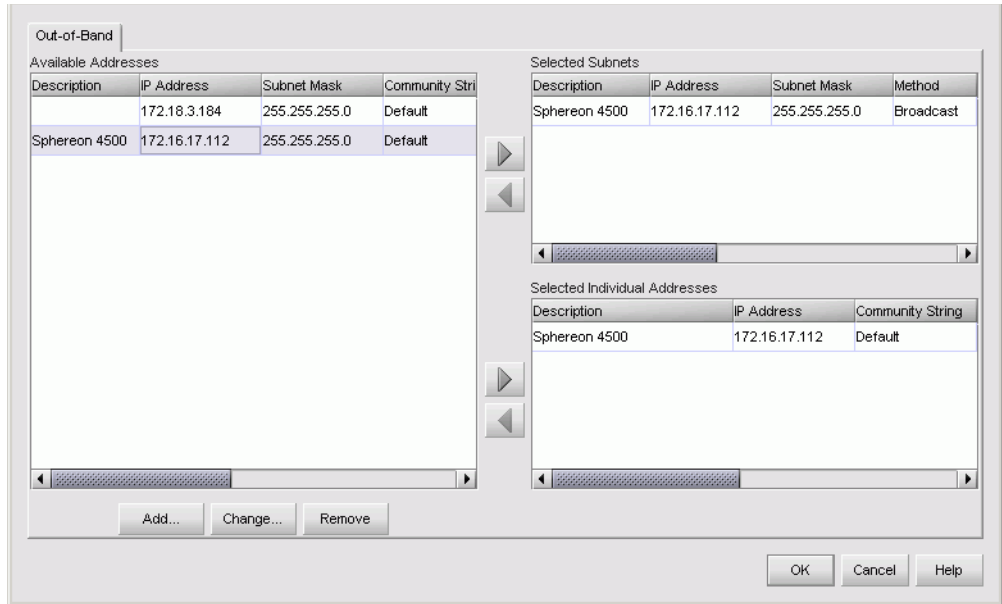
To reset director data to the factory default settings from the management server (Intrepid 6140 Element Manager application):

1. Notify the customer the director will be set offline. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. At the management server, open the SAN management application (SANavigator or EFCM).
3. Set the director offline ([Set the Director Online or Offline](#) on page 4-43).
4. At the SAN management application physical map, right-click the product icon representing the director for which a configuration file is to be reset to factory defaults, then select *Element Manager* from the pop-up menu. The application opens.
5. Select the *Reset Configuration* option from the *Maintenance* menu. The *Reset Configuration* dialog box displays ([Figure 4-67](#)).



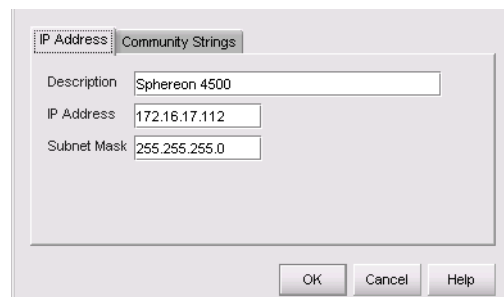
**Figure 4-67 Reset Configuration Dialog Box**

6. Click *Reset* to initiate the reset and close the dialog box.
7. The director IP address resets to the default address of **10.1.1.10**.
  - If the configured IP address (prior to reset) was the same as the default address, the director-to-management server Ethernet link is not affected and the procedure is complete.
  - If the configured IP address (prior to reset) was not the same as the default address, the director-to-management server Ethernet link drops and management server communication is lost. Continue to the next step.
8. To change the director IP address and restart the management server session, go to [step 10](#).
9. To restart a management server session using the default IP address of **10.1.1.10**:
  - a. Close the Intrepid 6140 Element Manager application and return to the SAN management application.
  - b. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset director, indicating the director is not communicating with the management server.
  - c. At the SAN management application, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays ([Figure 4-68](#)).



**Figure 4-68 Discover Setup Dialog Box**

- d. Select (highlight) the entry representing the reset director in the *Available Addresses* window and click *Change*. The *Domain Information* dialog box displays (Figure 4-69).



**Figure 4-69 Domain Information Dialog Box**

- e. Type **10.1.1.10** in the *IP Address* field and click *OK*. Entries at the *Discover Setup* dialog box reflect the new IP address.

- f. At the *Discover Setup* dialog box, click *OK*. Director-to-management server communication is restored and the procedure is complete.
10. Change the director IP address and restart the management server session as follows:
  - a. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset director, indicating director is not communicating with the management server.
  - a. Delete the icon representing the reset director. At the SAN management application, select the *Setup* option from the *Discover* menu. The *Discover Setup* dialog box displays (Figure 4-68).
  - b. Select (highlight) the entry representing the reset director in the *Available Addresses* window and click *Remove*.
  - c. At the *Discover Setup* dialog box, click *OK*. The director is no longer defined to the management server.
  - d. Change a director IP address through the maintenance port (*Task 4: Configure Director Network Information* on page 2-15).
  - e. Identify the switch to the SAN management application (*Subtask B: Identify the Director to the SAN Management Application* on page 2-42).
  - f. Director-to-management server communication is restored and the procedure is complete.

---

### Reset Configuration Data (SANpilot Interface)

To reset director data to the factory default settings from the SANpilot interface:

---

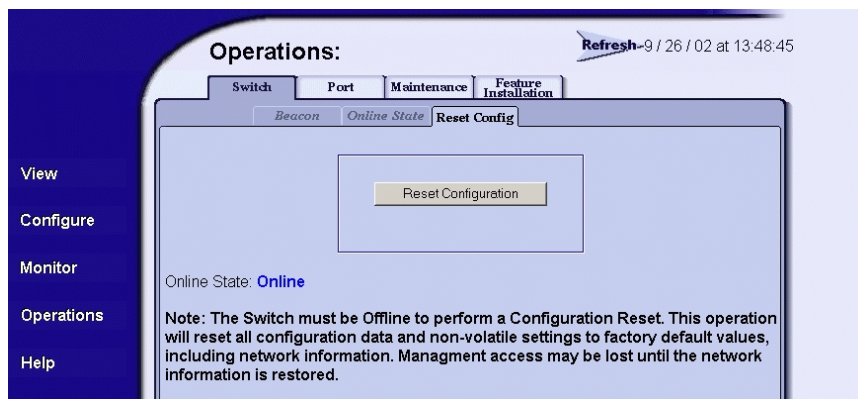
**NOTE:** When director configuration data is reset to factory default values, all optional features are disabled.

---

1. Notify the customer the director will be set offline. Ensure the customer system administrator quiesces Fibre Channel frame traffic through the director and sets attached devices offline.
2. Set the director offline (*Set the Director Online or Offline* on page 4-43).

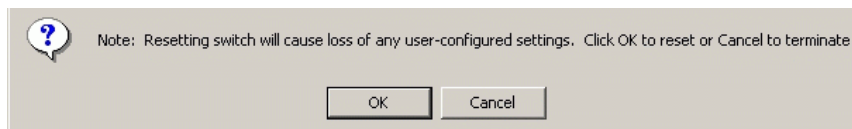


3. When the SANpilot interface opens, the *View* panel and *Switch* page appear as the default. At the *View* panel, select the *Operations* option at the left side of the panel. The *Operations* panel opens with the *Switch* page displayed.
4. Click the *Reset Config* tab. The *Switch* page displays with the *Reset Config* tab selected (Figure 4-70).



**Figure 4-70 Operations Panel (Switch Page with Reset Config Tab)**

5. Click *Reset Configuration*. A browser-specific message box displays (Figure 4-71).



**Figure 4-71 Browser-Specific Message Box**

6. Click *OK* to reset the configuration. The message **Your changes have been successfully activated** appears.
7. The director IP address resets to the default address of **10.1.1.10**.
  - If the configured IP address (prior to reset) was the same as the default address, the browser-to-director Internet connection is not affected and the procedure is complete.

- If the configured IP address (prior to reset) was not the same as the default address, the browser-to-director Internet connection drops and the SANpilot session is lost. Continue to the next step.
- 8. To change the director IP address and restart the SANpilot interface, see [Task 4: Configure Director Network Information](#) on page 2-15. To restart the SANpilot interface using the default IP address of **10.1.1.10**:
  - a. At the browser, enter the default IP address of **10.1.1.10** as the Internet URL. The *Enter Network Password* dialog box displays.
  - b. Type the default user name and password.

---

**NOTE:** The default user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- c. Click OK. The SANpilot interface opens with the *View* panel open and the *Switch* page displayed. The procedure is complete.

---

## Installing or Upgrading Software

This section describes the procedure to install or upgrade the SAN management application at the management server. The application includes the Intrepid 6140 Element Manager application.

The SAN management application shipped with the director is provided on the *EFC Management Applications* CD-ROM. Subsequent software versions for upgrading the director are provided to customers through an *EFC Management Applications* CD-ROM or through the McDATA website.

---

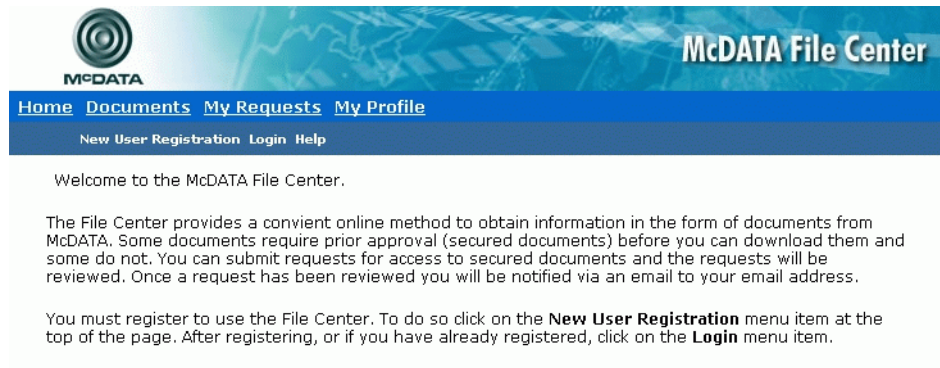
**NOTE:** When installing or upgrading a software version, follow all procedural information in release notes or EC instructions that accompany the software version. This information supplements information provided in this general procedure.

---

To install or upgrade the SAN management application and associated applications to the server:

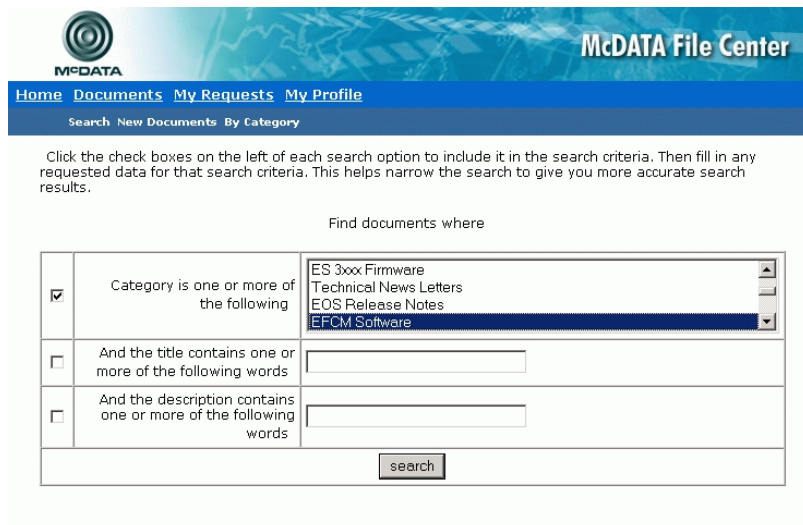
1. At the management server, close all SAN management sessions (local and remote) and exit all applications.

2. To install the new software version from the *EFC Management Applications* CD-ROM, go to [step 4](#).
3. To obtain a new software version from the McDATA File Center:
  - a. At a PC with Internet access, open the File Center home page ([Figure 4-72](#)). The uniform resource locator (URL) is <http://central.mcddata.com>.



**Figure 4-72** McDATA File Center Home Page

- b. Select (click) the *Login* option at the top of the home page. The *Login* page displays ([Figure 4-33](#)).
- c. Type the user name and password (assigned and registered while performing [Task 15: Register with the McDATA File Center](#) on page 2-120) and click *Login*. The *Welcome* page displays.
- d. Select (click) the *Documents* option at the top of the page. The *Find Documents* page displays ([Figure 4-73](#)).



**McDATA File Center**

[Home](#) [Documents](#) [My Requests](#) [My Profile](#)

Search New Documents By Category

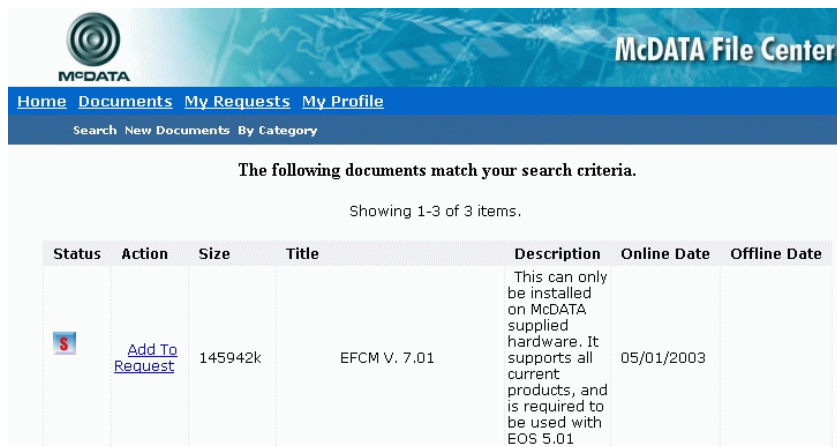
Click the check boxes on the left of each search option to include it in the search criteria. Then fill in any requested data for that search criteria. This helps narrow the search to give you more accurate search results.

Find documents where

<input checked="" type="checkbox"/>	Category is one or more of the following	ES 3xx Firmware Technical News Letters EOS Release Notes <b>EFCM Software</b>
<input type="checkbox"/>	And the title contains one or more of the following words	<input type="text"/>
<input type="checkbox"/>	And the description contains one or more of the following words	<input type="text"/>

**Figure 4-73 McDATA File Center (Find Documents Page)**

- e. Select (highlight) the *EFCM Software* option at the list box and click *Search*. The *Documents Match* page displays (Figure 4-74) with a list of software available for download.




**McDATA File Center**

[Home](#) [Documents](#) [My Requests](#) [My Profile](#)

Search New Documents By Category

The following documents match your search criteria.

Showing 1-3 of 3 items.

Status	Action	Size	Title	Description	Online Date	Offline Date
	<a href="#">Add To Request</a>	145942k	EFCM V. 7.01	This can only be installed on McDATA supplied hardware. It supports all current products, and is required to be used with EOS 5.01	05/01/2003	

**Figure 4-74 McDATA File Center (Documents Match Page)**

- f. Authorization to download a software version requires approval from the McDATA Solution Center. In the *Action* column adjacent to the desired software version, click *Add to Request*. The *Current Request* page displays (Figure 4-75).

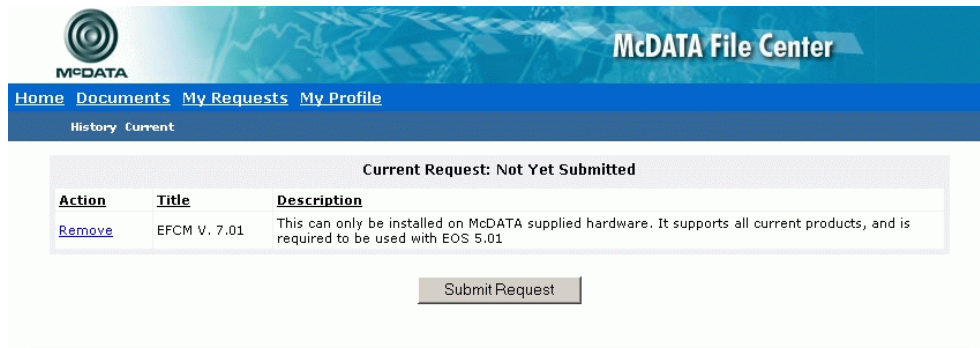


Figure 4-75 McDATA File Center (Current Request Page)

- g. Click *Submit Request*. The *Request Submitted* page displays and the request for approval is e-mailed to the McDATA Solution Center. Wait five to ten minutes for a response from McDATA, then select (click) the *My Requests* option at the top of the page. The *Request History* page displays (Figure 4-76) with the approved request.

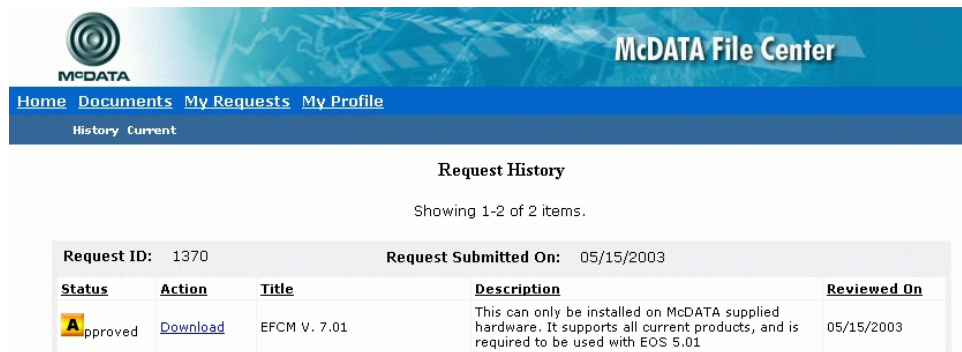
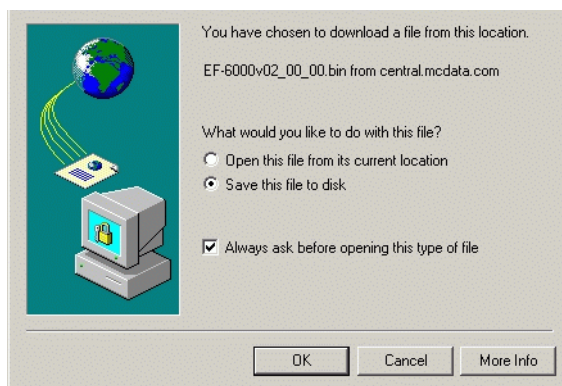


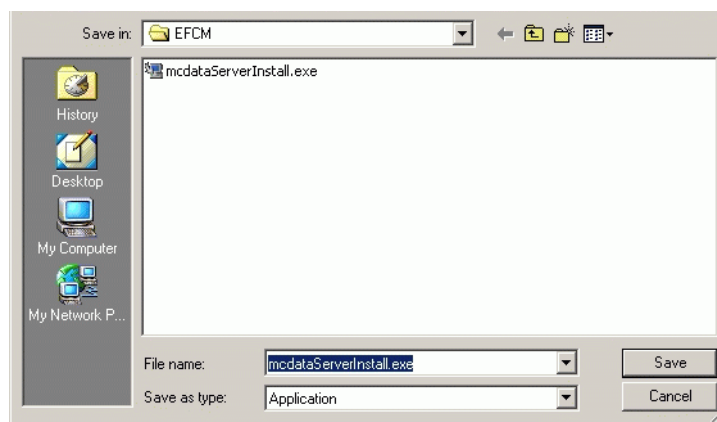
Figure 4-76 McDATA File Center (Request History Page)

- h. In the *Action* column adjacent to the approved request for the software version, click *Download*. The *File Download* dialog box displays (Figure 4-77).



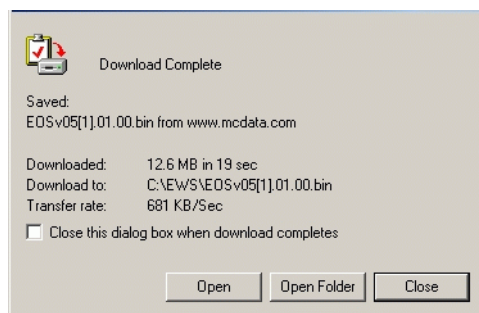
**Figure 4-77 File Download Dialog Box**

- i. Select the *Save this file to disk* radio button and click *OK*. The *Save As* dialog box appears (Figure 4-78).



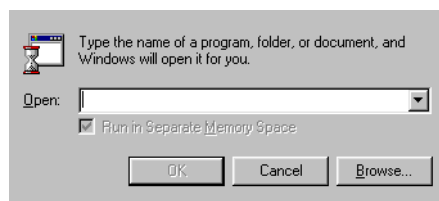
**Figure 4-78 Save As Dialog Box**

- j. At the *Save As* dialog box, ensure the correct directory path is specified at the *Save in* field and the correct file is specified in the *File name* field. Click *Save*.
- k. A *Download* dialog box displays, showing the estimated time remaining to complete the download. When the process finishes, the dialog box changes to a *Download complete* dialog box (Figure 4-79).



**Figure 4-79 Download Complete Dialog Box**

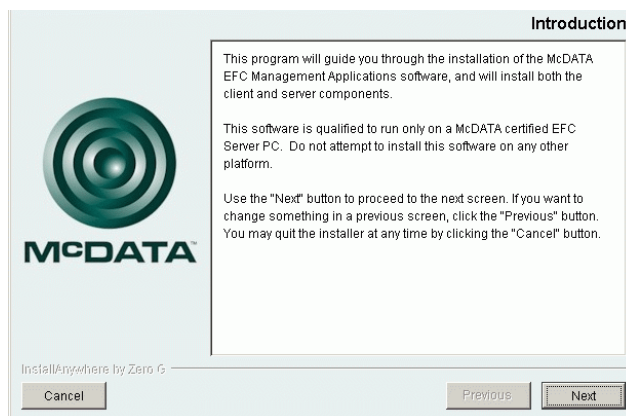
- l. Click *Close* to close the dialog box. The new firmware version is downloaded and saved to the PC hard drive.
  - m. At the PC, close the Internet session.
  - n. Transfer the firmware version file from the PC to the management server by diskette, CD-ROM, or other electronic means.
  - o. Go to [step 5](#).
4. Insert the *EFC Management Applications* CD-ROM into the CD-ROM drive of the management server.
5. At the management server Windows 2000 desktop, click *Start* at the left side of the task bar, then select *Run*. The *Run* dialog box ([Figure 4-80](#)) appears.



**Figure 4-80 Run Dialog Box**

6. At the *Run* dialog box, type **D:\mcdataServerInstall** in the *Open* field.
  7. Click *OK*. A series of message boxes appear as the *InstallAnywhere* third-party application prepares to install the EFC Manager software, followed by the *McDATA EFC Management Applications* dialog box ([Figure 4-81](#)).





**Figure 4-81 McDATA EFC Management Applications Dialog Box**

8. Follow the online instructions for the *InstallAnywhere* program. Click *Next*, *Install*, or *Done* as appropriate.
9. Power off and reboot the management server.
  - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.
  - b. Select the *Restart* option from the list box and click *OK*. The management server powers down and restarts. During the reboot the LAN connection between the management server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.
  - c. After the management server reboots, click *Login again*. The *VNC Authentication* screen displays.
  - d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays.

---

**NOTE:** The default TightVNC viewer password is **password**.

---

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the management server desktop. The *Log On to Windows* dialog box displays.



---

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action logs the user on to the browser-capable PC, not the management server.

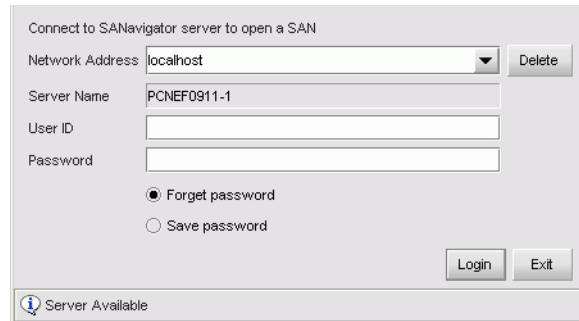
---

- f. Type the default Windows 2000 user name and password and click **OK**. The management server Windows 2000 desktop opens and the *SANavigator Log In* or *EFCM Log In* dialog box displays (Figure 4-82).

---

**NOTE:** The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---



The dialog box is titled "Connect to SANavigator server to open a SAN". It contains the following fields and controls:

- Network Address:** A drop-down menu showing "localhost" with a "Delete" button to its right.
- Server Name:** A text field containing "PCNEF0911-1".
- User ID:** An empty text field.
- Password:** An empty text field.
- Authentication Options:** Two radio buttons: "Forget password" (selected) and "Save password".
- Buttons:** "Login" and "Exit" buttons at the bottom right.
- Status Bar:** A message "Server Available" with an information icon on the left.

**Figure 4-82** SANavigator Log In or EFCM Log In Dialog Box

- g. Type the SAN management application default user name and password and select a server or IP address from the *Network Address* drop-down list.

---

**NOTE:** The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- h. Click *Login*. The application opens and the SANavigator or EFCM main window appears.



## Removal and Replacement Procedures (RRPs)

This chapter describes removal and replacement procedures (RRPs) used by authorized service representatives for all Intrepid 6140 Director field-replaceable units (FRUs). Do not perform a procedure in this chapter until a failure is isolated to a FRU. If fault isolation was not performed, go to [MAP 0000: Start MAP](#) on page 3-9.

### Factory Defaults

[Table 5-1](#) lists the defaults for the passwords, and IP, subnet, and gateway addresses.

**Table 5-1     Factory-Set Defaults**

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

---

## Procedural Notes

**NOTE:** The screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The following procedural notes are referenced as applicable. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a FRU repair, read the removal and replacement procedures for that FRU carefully and thoroughly to familiarize yourself with the procedures and reduce the possibility of problems or customer down time.
2. Follow all electrostatic discharge (ESD) procedures, **DANGER** and **CAUTION** statements, and statements listed in the preface of this manual.
3. After completing the steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.
4. After completing a replacement procedure, clear the event code reporting the failure and the event code reporting the recovery from the *Event Log* (at the management server or SANpilot interface), and extinguish the amber system error light-emitting diode (LED) at the director front bezel.

---

## Removing and Replacing FRUs

This section describes procedures to remove and replace director FRUs, along with a list of tools required to perform each procedure. In addition, the section provides:

- ESD information
- A list of concurrent FRUs. Concurrent FRUs can be removed and replaced while the director is powered on and operational.
- A list of nonconcurrent FRUs. Nonconcurrent FRUs can only be removed and replaced after the director is powered off.

See [Chapter 6, \*Illustrated Parts Breakdown\*](#) for FRU locations and part numbers.

---

## ESD Information

Follow all ESD procedures, **DANGER** statements, and **CAUTION** statements. When removing and replacing FRUs, always connect a grounding cable to the director chassis and wear an ESD wrist strap.

---

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

The ESD grounding points for the front of the chassis are located at the right and left sides of the chassis ([Figure 5-1](#)). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs.

If the director is not connected to facility power (and therefore not grounded), connect the ESD wrist strap to an approved bench grounding point instead of the chassis.

The ESD grounding point for the rear of the chassis is located next to the maintenance port ([Figure 5-1](#)). Touch the chassis once before performing any maintenance action, and once each minute while removing or replacing FRUs.

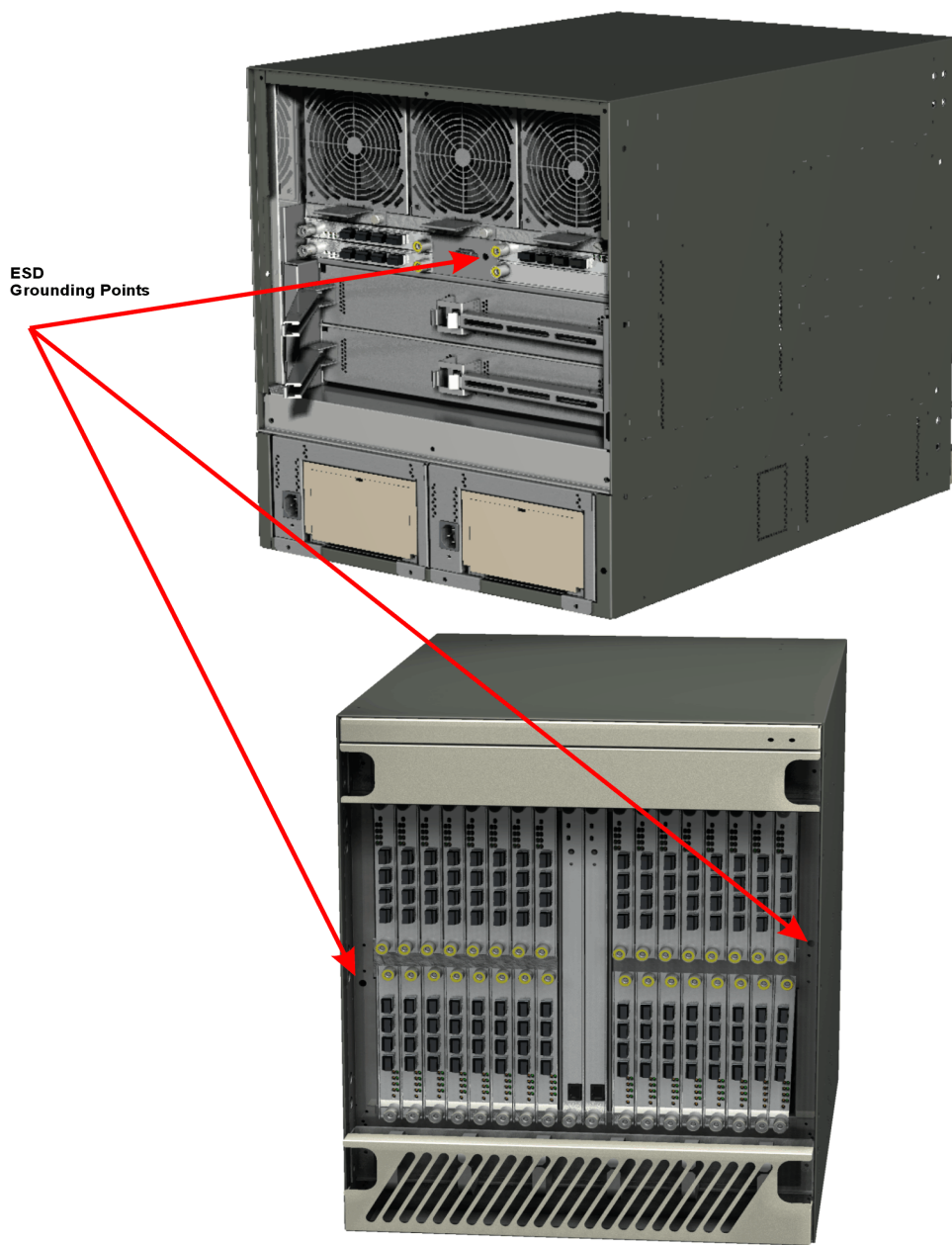


Figure 5-1 ESD Grounding Points

## Concurrent FRUs

[Table 5-2](#) lists the concurrent FRUs. Concurrent FRUs are removed and replaced while the director is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

**Table 5-2 Concurrent FRUs**

Concurrent FRU Name	ESD Precaution Requirement	Page
Control processor (CTP) card	Yes	<a href="#">5-6</a>
Universal port module (UPM) card	Yes	<a href="#">5-10</a>
10 Gbps port module (XPM) card	Yes	<a href="#">5-10</a>
Small form factor pluggable (SFP) optical transceiver	No	<a href="#">5-15</a>
10 Gbps form factor pluggable (XFP) optical transceiver	Yes	<a href="#">5-15</a>
UPM filler panel	No	<a href="#">5-19</a>
XPM filler blank	No	<a href="#">5-19</a>
Power supply	Yes	<a href="#">5-20</a>
AC module	Yes	<a href="#">5-24</a>
Fan module	Yes	<a href="#">5-27</a>
Power/System Error LED assembly	yes	<a href="#">5-30</a>
Serial crossbar (SBAR) assembly	Yes	<a href="#">5-31</a>

## Nonconcurrent FRU

[Table 5-3](#) lists the nonconcurrent FRU. A nonconcurrent FRU is removed and replaced after the director is powered off. The table also lists ESD precautions (yes or no) for the FRU, and references the page number of the removal and replacement procedure.

**Table 5-3 Nonconcurrent FRU**

Nonconcurrent FRU Name	ESD Precaution Requirement	Page
Backplane	Yes	<a href="#">5-35</a>

## RRP: CTP Card

Use the following procedures to remove or replace a CTP card (two cards in the director) with the backup CTP card operational. A list of tools required is provided.

**ATTENTION!** Do not remove and replace a CTP card if the backup CTP card is not fully operational and director power is on. The director IP address, configuration data, and other operating parameters will be lost.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

### Removal

To remove a CTP card:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative.

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
3. Identify the defective CTP card from the amber LED on the card or failure information at the management server *Hardware View*.
4. Disconnect the Ethernet local area network (LAN) cable from the RJ-45 connector on the card faceplate.



5. The CTP card is secured to the director chassis with two captive Allen screws. The bottom screw is spring-loaded and locks the CTP card in place. The top screw cams the CTP card into and out of the backplane.

**ATTENTION!** The torque tool supplied with the Intrepid 6140 Director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another McDATA product. Use of the wrong tool may overtighten and damage logic cards.

- a. Insert the torque tool into the locking Allen screw at the **bottom** of the card. Turn the screw counter-clockwise until the spring releases and the tool turns freely.
  - b. Insert the torque tool into the cam Allen screw at the **top** of the card (Figure 5-2). To unseat the CTP card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely.
6. Pull the CTP card from its card track and remove it from the director chassis. Place the card in an anti-static bag to provide ESD protection.

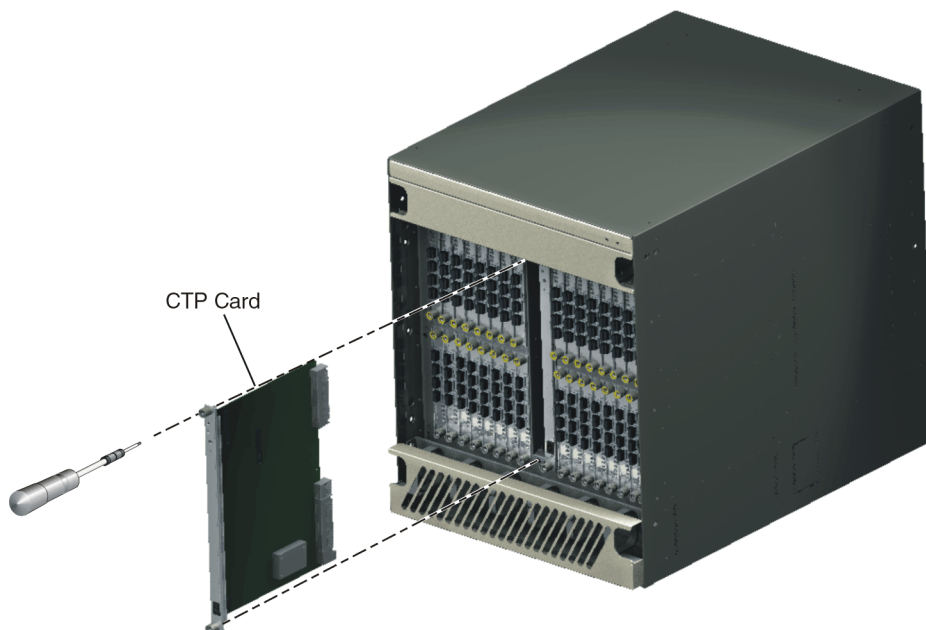


Figure 5-2 CTP Card Removal and Replacement

**Replacement**

To replace a CTP card:

1. Wait approximately 20 seconds after removal of the failed CTP card to begin this replacement procedure.
2. Remove the replacement card from its protective anti-static bag.
3. Hold the card by its stiffener and insert it in the chassis card track (Figure 5-2). The label identifying the card should be at the top. Verify the card is aligned in the card tracks, then slide it forward until it makes contact with the backplane.
4. Secure the CTP card:
  - a. Insert the torque tool into the cam Allen screw at the *top* of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.
  - b. Insert the torque tool into the locking Allen screw at the *bottom* of the card. Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
  - c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
5. After the replacement CTP card is installed, note the following:
  - When a CTP card with a different firmware version is installed in a director with an active CTP card, a synchronization process occurs. This process causes firmware from the active CTP card to be downloaded to the replacement CTP card. The process does not occur if both CTP cards have the same firmware version.
  - The synchronization process may take up to ten minutes (depending on director activity).

**ATTENTION!** Allow the synchronization process to complete. If the process is interrupted by a director power cycle or initial program load (IPL), or by removing the replacement CTP card, the card may be unusable due to partially-loaded firmware.

- If after ten minutes the replacement CTP card does not appear to be operational, perform the data collection procedure and return the failed replacement card to McDATA ([Collecting Maintenance Data](#) on page 4-39).

- Do not reinstall the failed replacement CTP card because this can corrupt director firmware. Obtain a new CTP card and perform this replacement procedure.
- 6. Verify that synchronization is complete by viewing the Event log.
- 7. Connect the Ethernet LAN cable to the RJ-45 connector on the faceplate of the replacement CTP card.
- 8. Disconnect the ESD wrist strap from the director chassis and your wrist.
- 9. Inspect the CTP card to ensure the amber LED is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
- 10. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure the following event codes appear in the log:
  - **410** - CTP card reset.
  - **416** - Backup CTP installed.
  - **422** - CTP firmware synchronization complete (only if the firmware versions on the two CTP cards are different).

If the event codes do not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

11. Perform one of the following to verify CTP card operation:
  - If at the management server, open the *Hardware View* and observe the CTP card graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate a CTP card failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
12. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).

13. If the customer requests the replacement CTP card be set as the active card, perform a FRU switchover. At the *Hardware View*, right-click the graphic representing the replacement card to open a menu, then select *Switchover*.
14. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:
    - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
    - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
    - c. Click *Clear Light*.
15. If necessary, close and lock the equipment cabinet door.

## RRP: Port Module Card (UPM and XPM)

Use the following procedures to remove or replace a UPM or XPM card. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).
- Fiber-optic protective plugs (provided with the director).
- Protective caps (provided with fiber-optic jumper cables).
- Fiber-optic cleaning kit.

### Removal

To remove a UPM or XPM card:

1. Notify the customer that all ports on the defective port card will be blocked. Ensure the customer system administrator quiesces Fibre Channel frame traffic through any operational ports on the card and sets attached devices offline.
2. If the director is installed in a stand-alone configuration, go to [step 4](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabriccenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.
3. To remove a rear-mounted FRU, remove the RFI shield.

---

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

4. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
5. Identify the defective port card from the amber LED on the card or failure information at the management server *Hardware View*.
6. Block communication to the defective port card ([Blocking and Unblocking Ports](#) on page 4-46).
7. If necessary, remove the RFI shield.
8. Disconnect the fiber-optic jumper cable from each port on the defective card as follows. Repeat this step for all four ports.
  - a. Pull the keyed LC connector free from the port optical transceiver.

---

**NOTE:** If name server zoning is implemented by port number, a change to the director fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

---

- b. Place a protective cap over the cable connector. If required, label jumper cables to ensure correct connections when the port card is replaced.

---

**ATTENTION!** When fiber-optic cables are disconnected from port card optical transceivers, ensure protective plugs are inserted into the receptacles. This prevents damage to sensitive components and prevents injury to the eye if the laser is viewed directly.

---

- c. Insert a protective plug into the optical transceiver.

---

**NOTE:** The spring-loaded (lock) Allen screws are colored yellow and are mounted near yellow "lock" symbols on the frame.

---

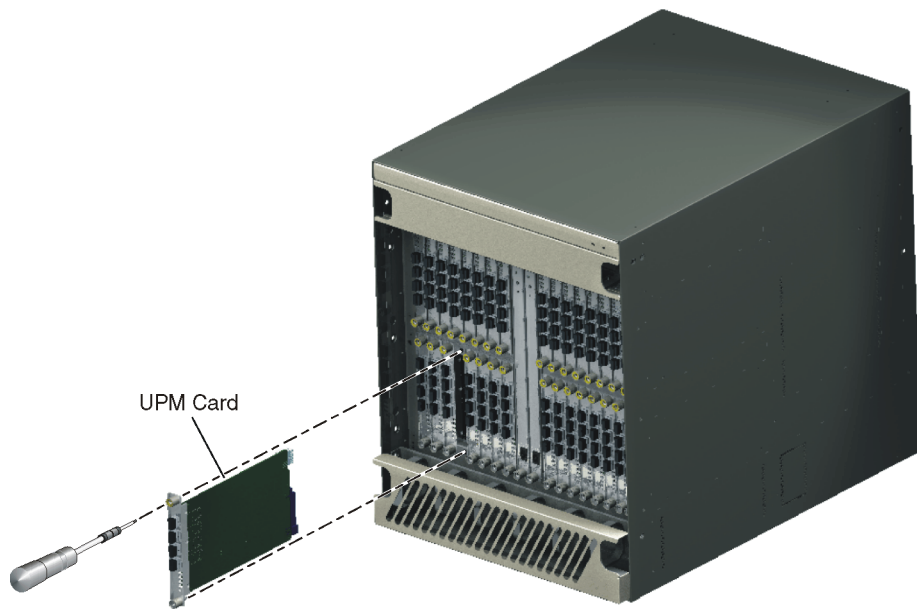
9. The port card is secured to the director chassis with two captive Allen screws. One screw (yellow) is spring-loaded and locks the port card in place. The other screw (uncolored) cams the port card into and out of the backplane.

---

**ATTENTION!** The torque tool supplied with the Intrepid 6140 Director is designed to tighten director logic cards and is set to release at a torque value of six inch-pounds. Do not use an Allen wrench or torque tool designed for use with another McDATA product. Use of the wrong tool may overtighten and damage logic cards.

---

- a. Insert the torque tool into the locking Allen screw (yellow). Turn the screw counter-clockwise until the spring releases and the tool turns freely.
  - b. Insert the torque tool into the cam Allen screw (uncolored). To unseat the port card and cam it out of the backplane, turn the screw counterclockwise until the tool turns freely ([Figure 5-3](#)).
10. Pull the port card from its card track and remove it from the director chassis. Place the card in an anti-static bag to provide ESD protection.



**Figure 5-3 UPM Card Removal and Replacement**

**Replacement** To replace a UPM or XPM card:

**NOTE:** The spring-loaded (lock) Allen screws are colored yellow and are mounted near yellow "lock" symbols on the frame.

1. Remove the replacement card from its protective anti-static bag.
2. Hold the card by its stiffener. Orient the card so that the locking Allen screw (yellow) on the card aligns with the yellow "lock" symbol on the frame. Verify that the card is aligned in the card tracks (Figure 5-3), then slide it forward until it makes contact with the backplane.
3. Secure the port card:
  - a. Insert the torque tool into the cam Allen screw (uncolored). Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card cams into the backplane connector.

- b. Insert the torque tool into the locking Allen screw (yellow). Turn the torque tool clockwise until you feel it release and hear a clicking sound. As the screw turns clockwise, the card locks into place.
    - c. Verify the card stiffener is flush with the front of the card cage and even with other director logic cards.
  4. Perform an external loopback test for all ports on the replacement port card ([Performing Port Diagnostic Loopback Tests](#) on page 4-30). If the test fails, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  5. Reconnect a fiber-optic jumper cable to each port on the card as follows. Inspect the label on the jumper cable to ensure the correct connection. Repeat this step for all four ports.
    - a. Remove the protective cap from the cable connector and the protective plug from the port optical transceiver. Store the cap and plug in a suitable location for safekeeping.
    - b. Clean the cable and port connectors ([Cleaning Fiber-Optic Components](#) on page 4-50).
    - c. Insert the keyed LC cable connector into port optical transceiver.
  6. If necessary, replace the RFI shield.
  7. Disconnect the ESD wrist strap from the director chassis and your wrist.
  8. Inspect the port card to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  9. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure the following event codes appear in the log:
    - **500** - Port card hot-insertion initiated.
    - **501** - Port card has been recognized.If an event code **501** does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  10. At the *Hardware View*, double-click the graphic representing the replacement card to open *Port Card View*. At the *Port Card View*:
    - a. Ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond).



- b. Verify port card information (FRU name, position, and state) is correct.

If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

11. Restore communication to the replacement port card and set the card online as directed by the customer ([Blocking and Unblocking Ports](#) on page 4-46). Inform the customer the port card is available for use.
12. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
13. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:
    - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
    - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
    - c. Click *Clear Light*.
14. If necessary, close and lock the equipment cabinet door.

## RRP: Optical Transceiver (SFP and XFP)

Use the following procedures to remove or replace an SFP or XFP optical transceiver from a UPM or XPM card. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- ESD grounding cable and wrist strap.
- Fiber-optic protective plug (provided with the director).

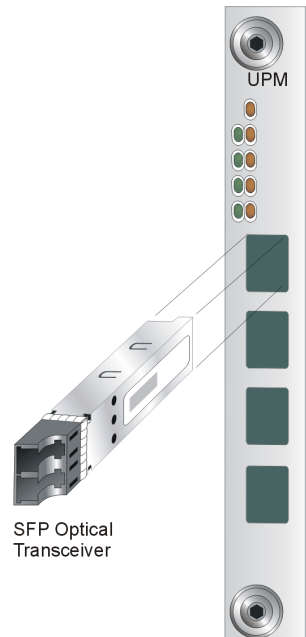
- Protective cap (provided with the fiber-optic jumper cable).
- Fiber-optic cleaning kit.

**Removal**

To remove an SFP or XFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer system administrator sets the attached device offline.
2. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabriccenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.
3. To remove a rear-mounted FRU, remove the RFI shield.
4. Identify the defective port transceiver from the amber LED on the port card or failure information at the management server *Port Card View*.
5. Block communication to the port ([Blocking and Unblocking Ports](#) on page 4-46).
6. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
7. Disconnect the fiber-optic jumper cable from the port:
  - a. Pull the keyed LC free from the port optical transceiver.
  - b. Place a protective cap over the cable connector.
8. Depending on the manufacturer, the optical transceiver may have a locking mechanism to secure the transceiver in the port receptacle, or the transceiver may have a pull tab to assist in removal.
  - a. If required, disengage the locking mechanism (usually at the left side of the transceiver) by squeezing the mechanism or pushing it toward the port receptacle.

- b. Grasp the pull tab or the optical transceiver frame and pull the transceiver from the port receptacle (Figure 5-4).



**Figure 5-4 SFP Optical Transceiver Removal and Replacement**

### Replacement

To replace an SFP or XFP optical transceiver:

1. Remove the transceiver from its packaging.
2. Insert the transceiver into the port receptacle (Figure 5-4).
3. Perform an external loopback test for the port (*Performing Port Diagnostic Loopback Tests* on page 4-30). If the test fails, go to *MAP 0000: Start MAP* on page 3-9 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
  - a. Remove the protective cap from the cable connector and the protective plug from the port optical transceiver. Store the cap and plug in a suitable location for safekeeping.
  - b. Clean the cable and port connectors (*Cleaning Fiber-Optic Components* on page 4-50).
  - c. Insert the keyed LC cable connector into port optical transceiver.

5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the port card with the replacement port transceiver to ensure all amber LEDs are extinguished. If any amber LEDs are illuminated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
7. If necessary, replace the RFI shield.
8. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure an event code **510** (SFP/XFP optics card hot-insertion initiated) appears in the log.

If an event code **510** does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

9. Perform one of the following to verify port card operation:
    - If at the management server, open the *Hardware View* and observe the port card graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
    - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate a port card failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
- If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
10. Restore communication to the port with the replacement transceiver as directed by the customer ([Blocking and Unblocking Ports](#) on page 4-46). Inform the customer the port is available for use.
  11. Perform one of the following to clear the system error (**ERR**) LED:

- If at the management server, open the *Hardware View* and:
  - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
  - b. Click the *Clear System Error Light* menu selection.
- If at a web browser connected to the SANpilot interface:

- a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
  - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
  - c. Click *Clear Light*.
12. If necessary, close and lock the equipment cabinet door.

## RRP: Filler Panel (UPM and XPM)

Use the following procedures to remove or replace a UPM or XPM filler panel. Filler panels cover and protect unused port card slots in the director chassis. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

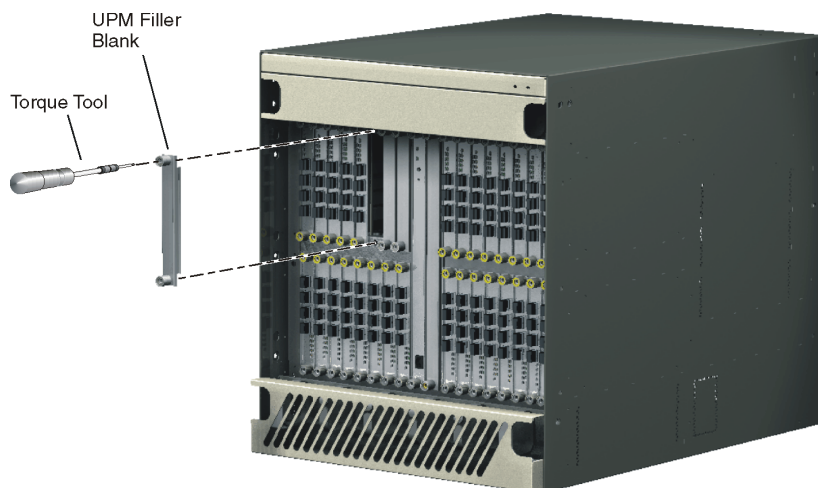
- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Torque tool and hex adapter (provided with the director).

### Removal

To remove a filler panel:

1. To remove a front-mounted FRU, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative.
2. To remove a rear-mounted FRU, remove the RFI shield.
3. Identify the filler panel to be removed.
4. The filler panel is secured to the director chassis with two captive Allen screws. Both screws are spring-loaded to lock the filler panel in place.
5. Insert the torque tool into each locking Allen screw ([Figure 5-5](#)). Turn each screw counter-clockwise until the spring releases and the tool turns freely.

6. Pull the filler panel out and remove it from the director chassis.



**Figure 5-5 Filler Panel Removal and Replacement**

### **Replacement**

To replace a filler panel:

1. Remove the filler panel from its packaging.
2. Hold the filler panel by its stiffener and insert it in the chassis card track ([Figure 5-5](#)).
3. To secure the filler panel, sequentially insert the torque tool into each locking Allen screw. Turn each screw clockwise until you feel the torque tool release and hear a clicking sound. As each screw turns clockwise, the filler panel locks into place.
4. Verify the filler panel stiffener is flush with the front of the card cage and even with other director logic cards.
5. If necessary, replace the RFI shield.
6. If necessary, close and lock the equipment cabinet door.

## **RRP: Power Supply**

Use the following procedures to remove or replace a power supply. A list of tools required is provided.

### **Tools Required**

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.

**Removal** To remove a power supply:

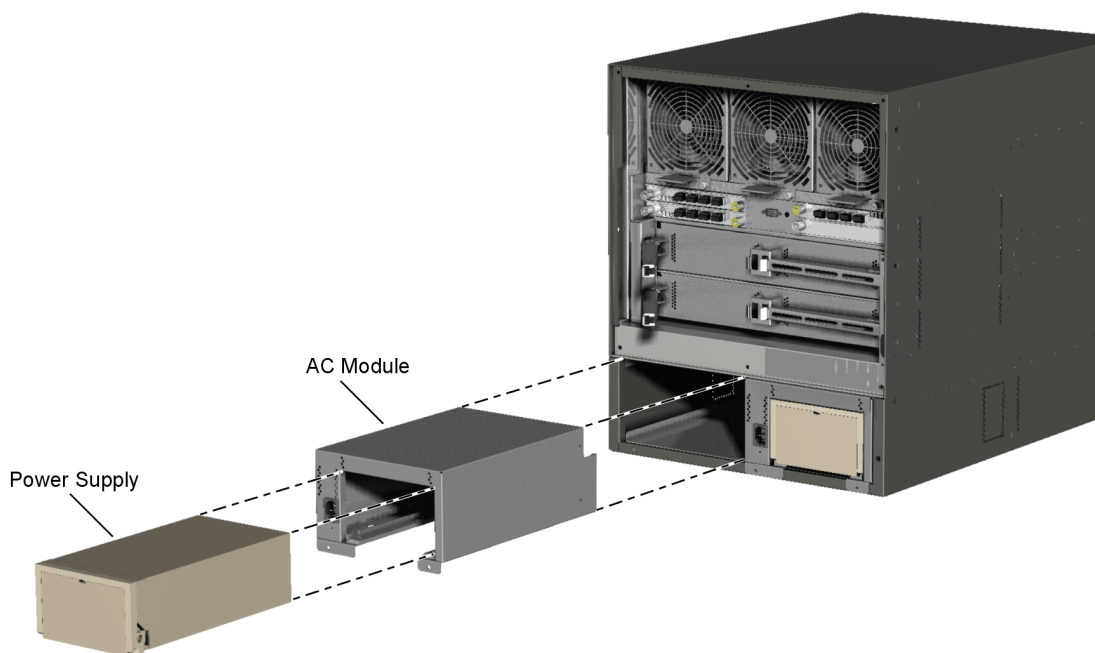
1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.

---

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
3. Identify the defective power supply from the extinguished green **PWR OK** LED on the supply or failure information at the management server *Hardware View*.
4. Use a flat-tip screwdriver to release the handle at the top of the power supply.



**Figure 5-6 Power Supply Removal and Replacement**

5. Pull the power supply from the director AC module (Figure 5-6). Support the power supply with one hand.
6. Place the power supply in an anti-static bag to provide ESD protection.

### **Replacement**

To replace a power supply:

1. Remove the replacement power supply from its protective anti-static bag.
2. Inspect the rear of the power supply for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new power supply.
3. Insert the power supply into the chassis guide of the AC module, then push the power supply toward the backplane to engage the connector pins.
4. Disconnect the ESD wrist strap from director chassis and wrist.



5. Inspect the power supply to ensure the green **PWR OK** LED is illuminated and all amber LEDs are extinguished. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
6. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure an event code **207** (power supply installed) appears in the log.  
  
If an event code **207** does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
7. Perform one of the following to verify power supply operation:
  - If at the management server, open the *Hardware View* and observe the power supply graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate a power supply failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
8. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
9. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:
    - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
    - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
    - c. Click *Clear Light*.
10. If necessary, close and lock the equipment cabinet door.

## RRP: AC Module

Use the following procedures to remove or replace the AC module. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.

### Removal

To remove the AC module:

1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.



### **DANGER**

***Disconnect the power cords.***

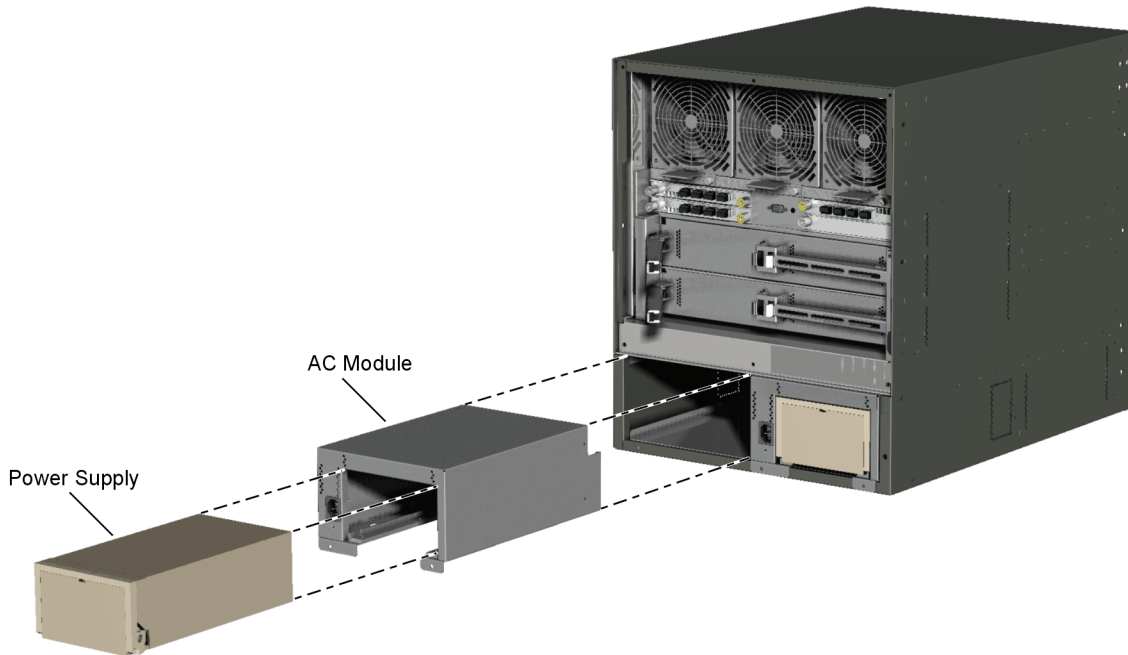
**ATTENTION!** Do not remove the power cord from the operational AC module.

2. Disconnect the power cord from the defective AC module.

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).

4. Remove the power supply from the defective AC module ([RRP: Power Supply](#) on page 5-20).
5. Remove the two panhead Phillips screws that secure the AC module to the director chassis ([Figure 5-7](#)).



**Figure 5-7 AC Module Removal and Replacement**

6. Pull the AC module out of the director chassis. Support the assembly with one hand.
7. Place the AC module in an anti-static bag to provide ESD protection.

### Replacement

To replace the AC module:

1. Remove the replacement AC module from its protective anti-static bag.
2. Inspect the printed wiring assembly (PWA) side of the AC module for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.

3. Position the AC module at the rear of the director chassis (Figure 5-7). Push the module toward the backplane to engage the connector pins.
4. Insert and tighten the two panhead Phillips screws that secure the AC module.
5. Replace the power supply (*RRP: Power Supply* on page 5-20).
6. Disconnect the ESD wrist strap from the director chassis and your wrist.
7. Connect the power cord to the AC module.
8. Verify that power-on self-tests (POSTs) complete and the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to *MAP 0000: Start MAP* on page 3-9 to isolate the problem.
9. Perform one of the following to verify AC module operation:
  - If at the management server, open the *Hardware View* and observe the AC module graphics to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to *MAP 0000: Start MAP* on page 3-9 to isolate the problem.
  - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate FRU failure. If a problem is indicated, go to *MAP 0000: Start MAP* on page 3-9 to isolate the problem.
10. Perform the data collection procedure (*Collecting Maintenance Data* on page 4-39).
11. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:
    - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.

- b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
- c. Click *Clear Light*.

12. If necessary, close and lock the equipment cabinet door.

## RRP: Fan Module

Use the following procedures to remove or replace a fan module. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.

### Removal

To remove a fan module:

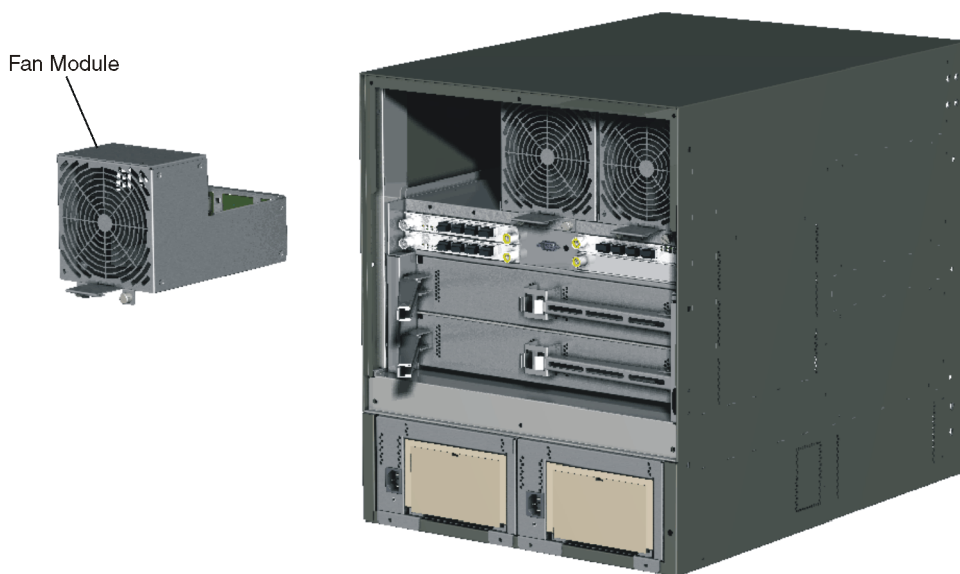
1. If the director is installed in a stand-alone configuration, go to [step 2](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.

**ATTENTION!** Do not remove a fan module unless a replacement module is available. Operation of the director with only two fan modules for an extended period may cause one or more thermal sensors to post event codes.

2. Remove the RFI shield.

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

3. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
4. Identify the defective fan module from the amber LED on the module or failure information at the management server *Hardware View*.
5. Two captive screws secure the fan module to the director chassis ([Figure 5-8](#)). Using a standard flat-tip screwdriver, loosen the captive screws.



**Figure 5-8 Fan Module Removal and Replacement**

6. Pull the module from the director. Support the fan module with one hand.
7. Place the fan module in an anti-static bag to provide ESD protection.

### **Replacement**

To replace the fan module:

1. Remove the replacement fan module from its protective anti-static bag.
2. Inspect the PWA on the underside of the fan module for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new fan module.

3. Position the fan module at the rear of the director chassis (Figure 5-8). Push the module toward the backplane to engage the connector pins. Support the fan module with one hand.
4. Using a standard flat-tip screwdriver, tighten the two captive screws that secure the fan module to the director chassis.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the fan module to ensure the amber LED is extinguished. If the LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
7. Replace the RFI shield.
8. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure an event code **321** (fan FRU inserted) appears in the log.

If an event code **321** does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

9. Perform one of the following to verify fan module operation:
  - If at the management server, open the *Hardware View* and observe the fan module graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate a fan module failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
10. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
11. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:

- a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
- b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
- c. Click *Clear Light*.

12. If necessary, close and lock the equipment cabinet door.

## RRP: Power/System Error LED Assembly

Use the following procedures to remove or replace the Power/System Error LED assembly. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.

### Removal

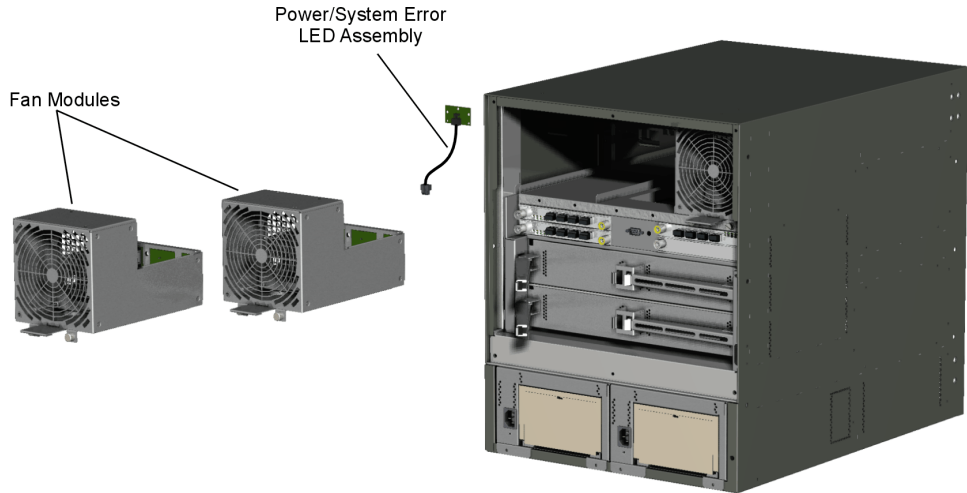
To remove the Power/System Error LED assembly:

1. Remove the RFI shield.

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

2. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
3. Remove only the center and *upper left* fan modules (viewed from the rear) ([RRP: Fan Module](#) on page 5-27).
4. Unplug the Power/System LED assembly cable from the backplane.
5. Remove the Power/System LED assembly ([Figure 5-9](#)).
6. Place the LED assembly in an anti-static bag to provide ESD protection.





**Figure 5-9 Power/System Error LED Assembly Removal and Replacement**

### Replacement

To replace the Power/System Error LED assembly:

1. Remove the replacement Power/System Error LED assembly from its protective anti-static bag.
2. Replace the Power/System LED assembly.
3. Plug the Power/System LED assembly cable into the backplane.
4. Replace the *center and upper left* fan modules (viewed from the rear) (*RRP: Fan Module* on page 5-27).
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Replace the RFI shield.

## RRP: SBAR Assembly

Use the following procedures to remove or replace an SBAR assembly. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).

- Standard flat-tip screwdriver.
- ESD grounding cable and wrist strap.
- Torque tool and hex adapter (provided with the director).

**Removal**

To remove an SBAR assembly:

1. If the director is installed in a stand-alone configuration, go to [step 3](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabricenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the rear door. Turn the tool counter-clockwise to unlock and open the door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet rear door as directed by the customer representative.
2. Remove the RFI shield.

---

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

---

3. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
4. Identify the defective SBAR assembly from the amber LED on the assembly or failure information at the management server *Hardware View*.
5. The SBAR assembly is secured to the director backplane with two handles (extractor levers) that snap lock ([Figure 5-10](#)). Open both handles.



**Figure 5-10 SBAR Assembly Removal and Replacement**

6. Using the handles, pull the SBAR assembly out of the director chassis. Support the assembly with one hand.
7. Place the SBAR assembly in an anti-static bag to provide ESD protection.

### **Replacement**

To replace an SBAR assembly:

1. Remove the replacement SBAR assembly from its protective anti-static bag.
2. Inspect the printed wiring assembly (PWA) side of the SBAR assembly for bent or broken connector pins that may have been damaged during shipping. If any pins are damaged, obtain a new assembly.
3. Orient the SBAR assembly (Figure 5-10). Insert the assembly into the director chassis guide, then push the assembly toward the backplane to engage the connector pins. Verify the assembly is flush and even with the other SBAR assembly in the director.
4. Close both handles.
5. Disconnect the ESD wrist strap from the director chassis and your wrist.
6. Inspect the assembly to ensure the amber LED is extinguished. If the amber LED is illuminated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.

7. Replace the RFI shield.
8. At the management server or at a web browser connected to the SANpilot interface, inspect the *Event Log*. Ensure the following event codes appear in the log:
  - **600** - SBAR card hot-insertion initiated.
  - **601** - SBAR card hot-insertion completed.

If an event code **601** does not appear in the log, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
9. Perform one of the following to verify SBAR operation:
  - If at the management server, open the *Hardware View* and observe the SBAR graphic to ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  - If at a web browser connected to the SANpilot interface, open the *Switch* tab at the *View* panel and ensure no amber LEDs illuminate that indicate an SBAR failure. If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
10. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
11. If the customer requests the replacement SBAR assembly be set as the active SBAR, perform a FRU switchover. At the *Hardware View*, right-click the graphic representing the replacement assembly to open a menu, then select *Switchover*.
12. Perform one of the following to clear the system error (**ERR**) LED:
  - If at the management server, open the *Hardware View* and:
    - a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
    - b. Click the *Clear System Error Light* menu selection.
  - If at a web browser connected to the SANpilot interface:
    - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.

- b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
- c. Click *Clear Light*.

13. If necessary, close and lock the equipment cabinet door.

## RRP: Backplane

Use the following procedures to remove or replace the backplane. A list of tools required is provided.

### Tools Required

The following tools are required to perform these procedures.

- Door key with 5/16-inch socket (provided with the FC-512 Fabricenter equipment cabinet).
- Torque tool and hex adapter (provided with the director).
- Standard flat-tip screwdriver.
- Standard cross-tip (Phillips) screwdriver.
- ESD grounding cable and wrist strap.
- Maintenance terminal (desktop or notebook PC) with:
  - The Microsoft Windows 98, Windows 2000, Windows Millennium Edition, or Windows NT 4.0 operating system.
  - RS-232 serial communication software (such as ProComm Plus or HyperTerminal). HyperTerminal is provided with Windows operating systems.
- Asynchronous RS-232 null modem cable (provided with the director).

### Removal

To remove the backplane:

1. At the *Hardware View*, double-click the graphic representing the director bezel (do not click a graphical FRU) to open the *Director Properties* dialog box. Record the director serial number. This number must be programmed into the replacement backplane.

If the director is not communicating with the management server (*Director Properties* dialog box is not available), obtain the serial number while performing [step 5](#).

2. Notify the customer that the director will be powered off. Ensure the customer system administrator quiets Fibre Channel frame traffic through the director and sets attached devices offline.
3. If the director is installed in a stand-alone configuration, go to [step 4](#). If the director is rack-mounted, perform one of the following:
  - If the director is installed in a McDATA-supplied FC-512 Fabriccenter equipment cabinet, insert the 5/16" door tool into the socket hole at the right top of the front door. Turn the tool counter-clockwise to unlock and open the door. Repeat this step to open the rear door.
  - If the director is installed in a customer-supplied equipment cabinet, unlock and open the cabinet front door as directed by the customer representative. Repeat this step to open the rear door.



### **DANGER**

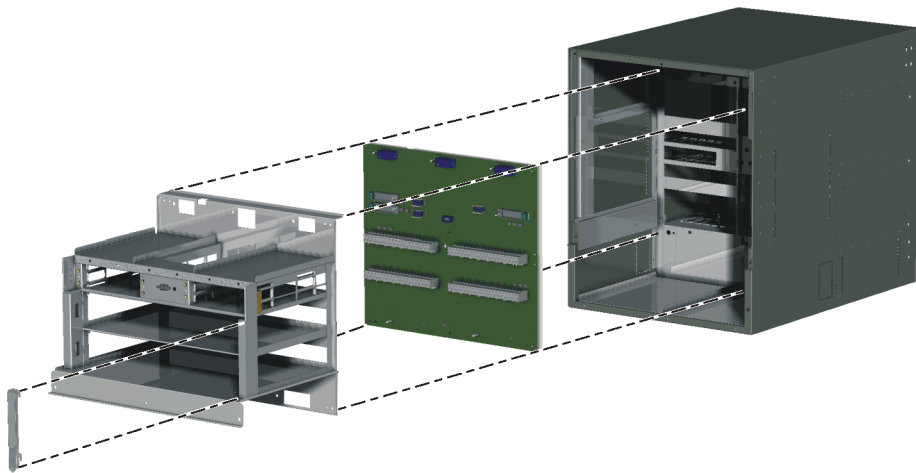
*Disconnect the power cords.*

4. Power off and unplug the director ([Power-Off Procedure](#) on page 4-52).
5. If necessary, record the director serial number.

**ATTENTION!** To avoid causing machine errors or damage while working on the director, follow ESD procedures by connecting a grounding cable to the director chassis and wearing an ESD wrist strap.

6. Remove the RFI shield.
7. Follow ESD procedures by attaching a wrist strap to the director chassis and your wrist ([Figure 5-1](#)).
8. Remove the CTP cards ([RRP: CTP Card](#) on page 5-6).
9. Remove the port cards ([RRP: Port Module Card \(UPM and XPM\)](#) on page 5-10).
10. Remove the power supplies ([RRP: Power Supply](#) on page 5-20).
11. Remove the AC modules ([RRP: AC Module](#) on page 5-24).
12. Remove the fan modules ([RRP: Fan Module](#) on page 5-27).

13. Remove the SBAR assemblies (*RRP: SBAR Assembly* on page 5-31).
14. Unplug the Power/System LED assembly cable from the backplane.
15. The card cage and backplane are secured to the director chassis with 6 panhead Phillips screws. Use a standard Phillips screwdriver to remove these screws.
16. Remove the card cage and backplane assembly (*Figure 5-11*).



**Figure 5-11 Backplane Removal and Replacement**

17. Disconnect the maintenance port cable from the backplane.
18. The backplane is secured to the card cage with 7 panhead Phillips screws. Use a standard Phillips screwdriver to remove these screws.
19. Remove the backplane (PWA and frame as one FRU) from the card cage. Place the backplane in an anti-static bag to provide ESD protection.

### Replacement

To replace the backplane and all FRUs disconnected from the backplane:

1. Remove the replacement backplane from its protective anti-static bag. Inspect the backplane PWA to ensure no connector pins are damaged.

2. Align the guide pins on the back of the backplane with the alignment holes in the card cage.
3. While holding the backplane in place, insert and hand tighten one of the top center panhead Phillips screws.
4. Insert and hand tighten the remaining six panhead Phillips screws.
5. Using a standard Phillips screwdriver, tighten the 7 panhead screws that secure the backplane to the card cage. Tighten the screws alternately from bottom to top and from side to side.
6. Connect the maintenance port cable.
7. Replace the card cage and backplane in the director chassis. with 6 panhead Phillips screws. Use a standard Phillips screwdriver to replace the 6 panhead Phillips screws.
8. Plug the Power/System LED assembly cable into the backplane.
9. Replace the SBAR assemblies (*RRP: SBAR Assembly* on page 5-31).
10. Replace the fan modules (*RRP: Fan Module* on page 5-27).
11. Replace the AC modules (*RRP: AC Module* on page 5-24).
12. Replace the power supplies (*RRP: Power Supply* on page 5-20).
13. Replace the port cards (*RRP: Port Module Card (UPM and XPM)* on page 5-10).
14. Replace the CTP cards (*RRP: CTP Card* on page 5-6).
15. Disconnect the ESD wrist strap from the director chassis and your wrist.
16. Replace the RFI shield.
17. Connect the power cords and power on the director (*Power-On Procedure* on page 4-51).
18. Verify that POSTs complete and the green power LED on the front bezel, green LED on the active CTP card, and green **PWR OK** LEDs on both power supplies remain illuminated. If a problem is indicated, go to *MAP 0000: Start MAP* on page 3-9 to isolate the problem.
19. Reprogram the replacement backplane with the original director serial number:



- a. Remove the protective cap from the 9-pin maintenance port at the rear of the director (a flat-tip screwdriver may be required). Connect the 9-pin end of the RS-232 modem cable to the port.
  - b. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
  - c. Power on the maintenance terminal. Use the following settings.
    - Bits per second - 115200.
    - Data bits - 8.
    - Parity - None.
    - Stop bits - 1.
    - Flow control - Hardware.

When the parameters are set, click *OK*. The *HyperTerminal* dialog box displays.
  - d. At the **>** prompt, type the maintenance-level password (the default is **level-2**) and press **Enter**. The password is case sensitive. The *HyperTerminal* dialog box displays with a **C>** prompt at the top of the window.
  - e. Type the command **oem #####**, where **#####** is the original director serial number recorded in [step 1](#) or [step 5](#) of the removal procedure.
  - f. Select *Exit* from the *File* pull-down menu to close the *HyperTerminal* application.
20. Initial machine load (IML) the director. At the front of the director, press and hold the white IML button on the faceplate of the active CTP card (green LED illuminated) for three seconds.
  21. At the management server *Hardware View*, observe all FRU graphics and ensure no alert symbols appear that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to [MAP 0000: Start MAP](#) on page 3-9 to isolate the problem.
  22. Perform the data collection procedure ([Collecting Maintenance Data](#) on page 4-39).
  23. Perform one of the following to clear the system error (**ERR**) LED:
    - If at the management server, open the *Hardware View* and:

- a. Right-click the front panel bezel graphic (away from a FRU) to open a menu.
  - b. Click the *Clear System Error Light* menu selection.
- If at a web browser connected to the SANpilot interface:
  - a. Click the *Switch* tab at the *Operations* panel. The *Operations* panel opens with the *Switch* page displayed.
  - b. Click the *Sys Err Light* tab. The *Switch* page displays with the *Sys Err Light* tab selected. A **System Error Light is ON** message displays on the page.
  - c. Click *Clear Light*.
24. If necessary, close and lock the equipment cabinet doors.

This chapter provides an illustrated parts breakdown for all Intrepid 6140 Director field-replaceable units (FRUs) and parts. Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the director disassembly sequence for clarity. Illustrated FRUs and parts are numerically keyed to associated parts lists. The parts lists include McDATA part numbers, descriptions, and quantities.

An (\*ESD\*) symbol precedes the description of a FRU containing electrostatic discharge (ESD) sensitive components. Handle ESD-labelled FRUs in accordance with caution statements in this manual.

## Front-Accessible FRUs

Figure 6-1 illustrates the front-accessible FRUs and Table 6-1 is the parts list. The table includes reference numbers to Figure 6-1, part numbers, descriptions, and quantities.

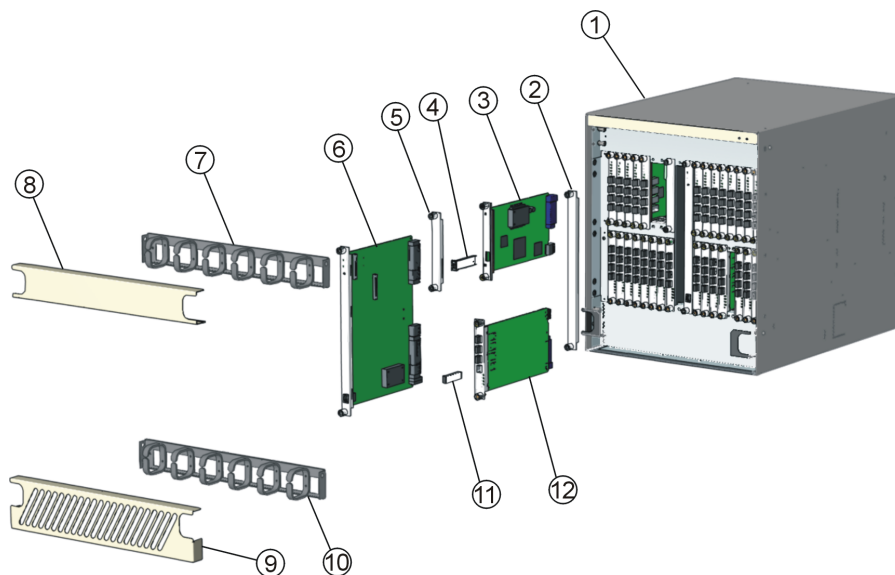


Figure 6-1 Front-Accessible FRUs

Table 6-1 Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
6-1-1	Reference	Base assembly, Intrepid 6140 Director	1
-2	reference	Filler panel, CTP	0 to 1
-3		(*ESD*) Printed wiring assembly, 10 Gbps port module (XPM), 1-port, LC, (pluggable optics not included)	
-4	803-000100-850	(*ESD*) XFP transceiver, optical, shortwave (SW) laser, 10.625 Gbps, 850 nm, LC	
-4	803-000100-313	(*ESD*) XFP transceiver, optical, longwave (LW) laser, 10.625 Gbps, 1300 nm, LC	
-5	002-002230-100	Filler panel, UPM or XPM	1 to 17
-6	470-000437-401	(*ESD*) Printed wiring assembly, control processor (CTP)	2
-7	Reference	Bracket, d-ring (cable organizer feature), upper	1
-8	Reference	Cover, top cable	1
-9	Reference	Cover, lower cable	1
-10	Reference	Bracket, d-ring (cable organizer feature), lower	1
-11	803-000064-386	(*ESD*) SFP transceiver, optical, shortwave (SW) laser, 2.1250 Gbps, 850 nm, LC	0 to 140
-11	803-000065-313	(*ESD*) SFP transceiver, optical, longwave (LW) laser, 2.1250 Gbps, 1300 nm, LC	0 to 140
-12	002-002669-000	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (pluggable optics not included)	16 to 35

## Rear-Accessible FRUs

Figure 6-2 and Figure 6-3 illustrate the rear-accessible FRUs, and Table 6-2 and Table 6-3 are the parts lists. The table includes reference numbers to Figure 6-2, part numbers, descriptions, and quantities.

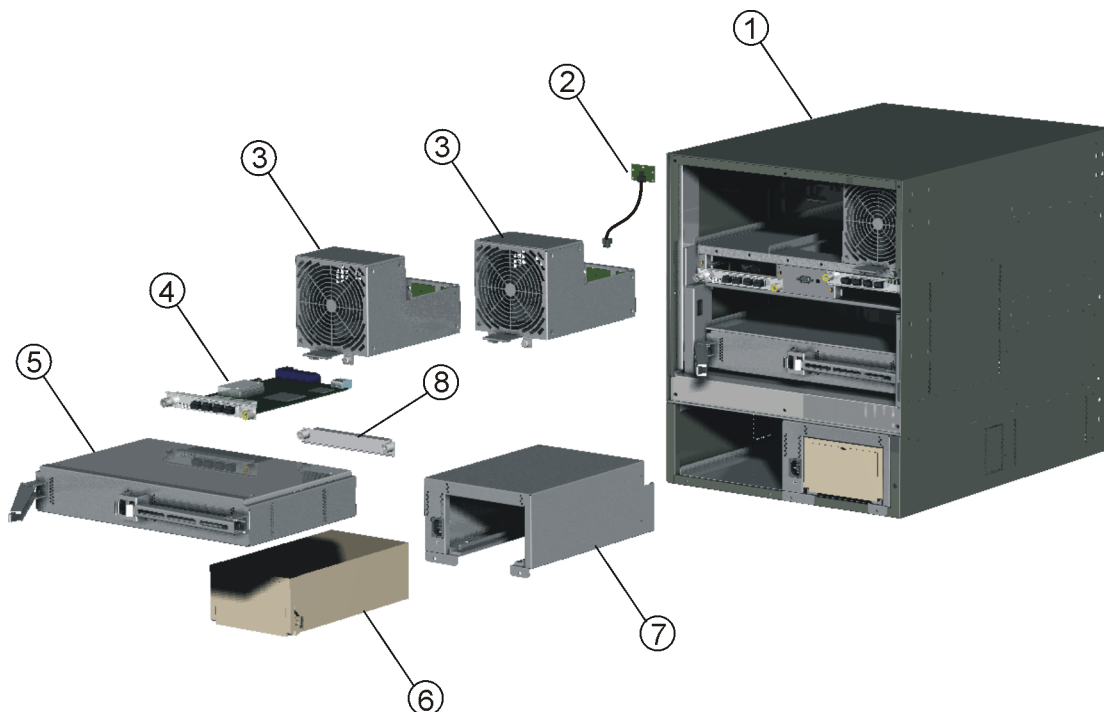
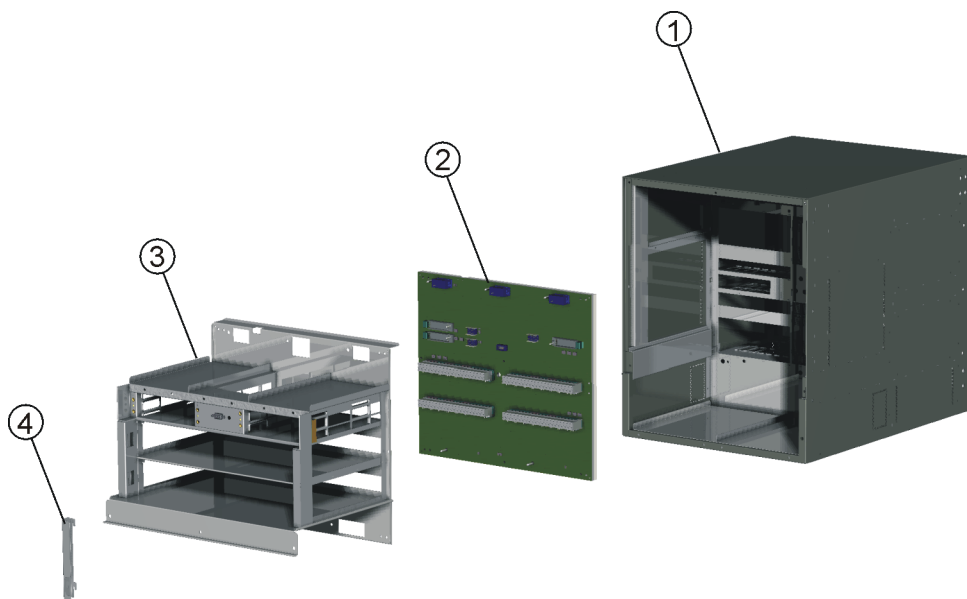


Figure 6-2 Rear-Accessible FRUs (Part 1)

**Table 6-2 Rear-Accessible FRU Parts List (Part 1)**

Ref.	Part Number	Description	Qty.
6-2-1	Reference	Base assembly, Intrepid 6140 Director	1
-2	470-000466-100	(*ESD*) LED assembly, power/system error	1
-3	476-000462-102	(*ESD*) Fan module	3
-4	See <a href="#">Table 6-1</a>	(*ESD*) Printed wiring assembly, universal port module (UPM), 4-port, LC (pluggable optics not included)	16 to 35
-xx	See <a href="#">Table 6-1</a>	(*ESD*) Printed wiring assembly, 10 Gbps port module (XPM), 1-port, LC, (pluggable optics not included)	
--5	475-000471-201	(*ESD*) Printed wiring assembly, serial crossbar (SBAR)	2
-6	721-000058-001	(*ESD*) Power supply, 180 - 264 VAC, 48 VDC	2
-7	002-002489-100	(*ESD*) AC module (Power distribution assembly)	2
-8	See <a href="#">Table 6-1</a>	Filler panel, UPM or XPM	1 to 17



**Figure 6-3 Rear-Accessible FRUs (Part 2)**

**Table 6-3 Rear-Accessible FRU Parts List (Part 2)**

Ref.	Part Number	Description	Qty.
6-2-1	Reference	Base assembly, Intrepid 6140 Director	1
-2	476-000435-300	(*ESD*) Printed wiring assembly, backplane	1
-3	Reference	Cage assembly, rear card	1
-4	Reference	Retainer, rear cable guide	1



## Miscellaneous Parts

Figure 6-4 illustrates the miscellaneous parts, and Table 6-4 is the parts list. The table includes reference numbers to Figure 6-4, part numbers, descriptions, and quantities.

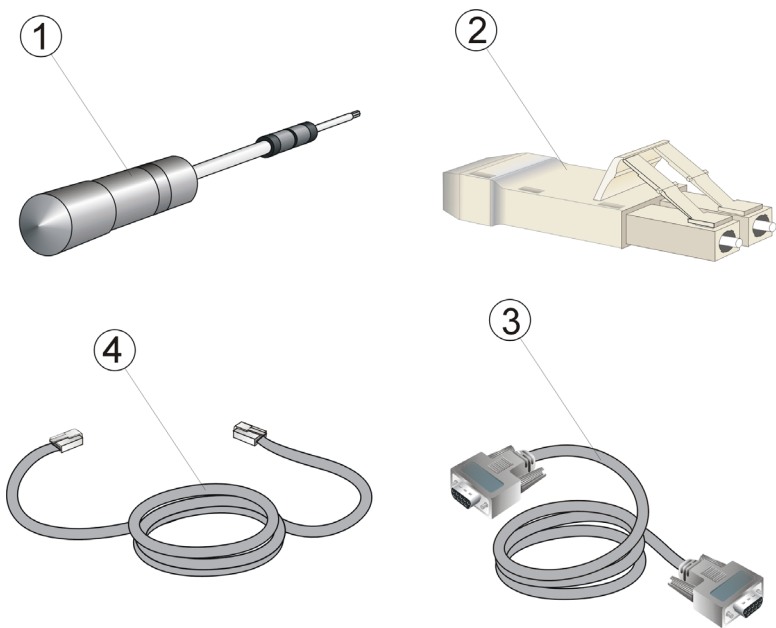


Figure 6-4 Miscellaneous Parts

**Table 6-4     Miscellaneous Parts**

Ref.	Part Number	Description	Qty.
6-1	002-002317-000	Torque driver with 5/32 in. bit	1
-2	803-000057-000	Loopback plug, LC, MM (50/125) (#1148)	1
-2	803-000057-001	Loopback plug, LC, SM (9/125) (blue) (#1149)	1
-3	801-000039-000	Null modem cable, DB9F-DB9F	1
-4	801-000035-010	Ethernet cable, 10 ft.	1

# Power Cords and Receptacles

Figure 6-5 illustrates the optional power cords and receptacles and Table 6-5 is the parts list. The table includes reference numbers to Figure 6-5, feature numbers, and descriptions.

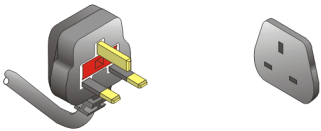
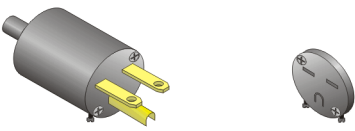
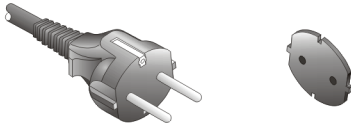
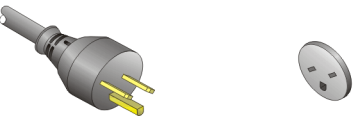
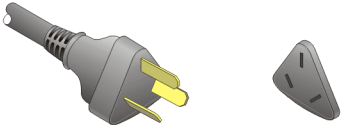

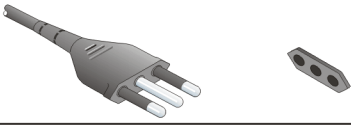
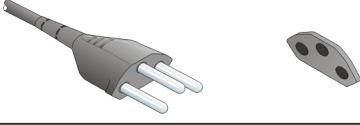

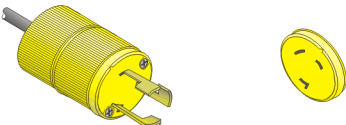
1		6,10,14	
2		7	
3		8	
4		9	
5		11,12,13	

Figure 6-5 Power Cords and Receptacles

Table 6-5 Power Cord and Receptacle List

Ref.	Part Number	Description	Feature
-1	806-000004-001	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
-2	806-000005-001	Power cord, AC, European Community CEE 7/7 straight, 250 volts, 10 amps, 2.5 meters Receptacle: CEE 7	1013
-3	806-000006-001	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
-4	806-000027-000	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
-5	806-000029-000	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
-6	806-000030-000	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
-7	806-000033-000	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
-8	806-000034-000	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
-9	806-000037-000	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
-10	806-000038-000	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027
-11	806-000040-000	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028

Table 6-5     **Power Cord and Receptacle List (*continued*)**

Ref.	Part Number	Description	Feature
-12	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016
-13	806-000042-000	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1029
-14	806-000043-000	Power cord, AC, Japan NEMA 6-15P straight, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA 6-15R	None



This appendix lists information and error messages that appear in pop-up message boxes at the Intrepid 6140 Element Manager applications.

## Intrepid 6140 Element Manager Messages

This section lists Intrepid 6140 Element Manager information and error messages in alphabetical order.

### A

<b>Message</b>	<b>A preferred path already exists between this Source Port and this Destination Domain ID. Please reconfigure the desired path.</b>
<b>Description</b>	For any source port, only one path may be defined to each destination domain ID.
<b>Action</b>	On the <i>Add/Change Preferred Path</i> Dialog box, change the Preferred Path.
<b>Message</b>	<b>Activating this configuration will overwrite the current configuration.</b>
<b>Description</b>	Confirmation to activate a new address configuration.
<b>Action</b>	Click <i>Yes</i> to confirm activating the new address configuration or <i>No</i> to cancel the operation.

<b>Message</b>	<b>All configuration names must be unique.</b>
<b>Description</b>	All address configurations must be saved with unique names.
<b>Action</b>	Save the configuration with a different name that is unique to all saved configurations.
<b>Message:</b>	<b>All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?</b>
<b>Description:</b>	Occurs when FPM cards are installed in the director and director speed is being set to 2 Gb/sec in the <i>Configure Operating Parameters</i> dialog box.
<b>Action:</b>	Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec.
<b>Message</b>	<b>All port names must be unique.</b>
<b>Description</b>	A duplicate port name was entered. Every configured port name must be unique.
<b>Action</b>	Reconfigure the port with a unique name.
<b>Message</b>	<b>Another Element Manager is currently performing a firmware install.</b>
<b>Description</b>	Only one firmware install to a specific director or switch can take place at a time.
<b>Action</b>	Wait for the firmware install to complete and retry the operation.
<b>Message</b>	<b>Are you sure you want to delete firmware version?</b>
<b>Description</b>	Requesting confirmation to delete the firmware version. Firmware library can hold eight firmware versions.
<b>Action</b>	Click <i>Yes</i> to confirm the firmware deletion or <i>No</i> to cancel the operation.



<b>Message</b>	<b>Are you sure you want to delete this address configuration?</b>
<b>Description</b>	Confirmation to delete the selected address configuration.
<b>Action</b>	Click <i>Yes</i> to confirm the deletion of the address configuration or <i>No</i> to cancel the operation.
<b>Message</b>	<b>Are you sure you want to send firmware version?</b>
<b>Description</b>	Requesting confirmation to send a firmware version.
<b>Action</b>	Click <i>Yes</i> to confirm the firmware send or <i>No</i> to cancel the operation.

## C

<b>Message</b>	<b>Cannot change port type while Management Style is FICON, without SANtegrity Feature. Please contact your sales representative.</b>
<b>Description</b>	Firmware level is below 6.0 and user attempted to change a port type in the <i>Configure Ports</i> dialog box while FICON management style is enabled, but the optional SANtegrity Binding feature is not installed.
<b>Action</b>	Informational message. If the firmware is below 6.0, install SANtegrity Binding feature before changing port types in the <i>Configure Ports</i> dialog box while using FICON Management style.
<b>Message</b>	<b>Cannot create partition &lt;partition number&gt; while FICON Management Server is enabled.</b>
<b>Description</b>	The user has moved slots into a partition while the FMS server is enabled.
<b>Action</b>	Disable FMS before moving slots into a partition.
<b>Message</b>	<b>Cannot disable switch binding while Enterprise Fabric Mode is active and the switch is online.</b>

<b>Description</b>	The user attempted to disable switch binding through the <i>Switch Binding Change State</i> dialog box, but <i>Enterprise Fabric Mode</i> is enabled.
<b>Action</b>	Either disable <i>Enterprise Fabric Mode</i> using the <i>Enterprise Fabric Mode</i> dialog box at the SAN management application, or set the director or switch offline to disable switch binding.
<b>Message</b>	<b>Cannot disable Insistent Domain ID while fabric binding is active.</b>
<b>Description</b>	The user attempted to disable the <i>Insistent Domain ID</i> parameter through the <i>Configure Switch Parameters</i> dialog box, but fabric binding is enabled.
<b>Action</b>	Disable fabric binding through the <i>Fabric Binding</i> dialog box before disabling the parameter.
<b>Message</b>	<b>Cannot enable beaconing on a failed FRU.</b>
<b>Description</b>	Occurs when selecting <i>Enable Beaconing</i> option for a failed FRU.
<b>Action</b>	Replace FRU and enable beaconing or enable beaconing on operating FRU.
<b>Message</b>	<b>Cannot enable beaconing while the system error light is on.</b>
<b>Description</b>	Beaconing cannot be enabled while the system error LED is on.
<b>Action</b>	Select <i>Clear System Error Light</i> from the <i>Products</i> menu to clear the error light, then enable beaconing.
<b>Message</b>	<b>Cannot enable OpenTrunking while Enterprise Fabric Mode is active and the switch is offline.</b>
<b>Description</b>	<i>Enterprise Fabric Mode</i> is active, the director or switch is offline, and a user is attempting to enable OpenTrunking feature. This message displays only if the feature is installed.
<b>Action</b>	Perform one of the following:

- Disable *Enterprise Fabric Mode* by selecting the appropriate fabric at the fabric tree portion of the *Fabrics* view. Open the *Enterprise Fabric Mode* dialog box, click *Start*, and follow the prompts to disable the feature.
- Set the director or switch online through the *Set Online State* dialog box.

**Message**      **Cannot have E\_Ports if Management Style is FICON unless SANtegrity feature is installed. Contact your sales representative.**

**Description**      Firmware level is below 6.0 and user attempted to change Open Systems to FICON with E\_ports enabled but without the SANtegrity feature installed.

**Action**      Informational message. If the firmware is below 6.0, if you install SANtegrity Binding feature before changing to FICON Management style, the E\_Ports will remain E\_Ports when you change to FICON Management style. If SANtegrity Binding feature is not installed, setting a director to FICON Management style will change all E\_Ports to G\_Ports.

**Message**      **Cannot have spaces in field.**

**Description**      Spaces are not allowed in this field.

**Action**      Remove the spaces or retype the field without spaces.

**Message**      **Cannot install firmware to a director with a failed CTP card.**

**Description**      Firmware cannot be installed on a director with a failed CTP card.

**Action**      Replace the failed CTP card and retry the firmware install to the director.

**Message**      **Cannot modify director/switch speed. Port speeds cannot be configured at a higher data rate than the director/switch speed.**

**Description**      Port speeds cannot be configured at a higher data rate than the director speed. This displays when you set the director speed to 1

Gb/sec through the *Configure Operating Parameters* dialog box and at least one of the ports is running at 2 Gb/sec.

**Action** Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the *Configure Ports* dialog box.

**Message** Cannot perform this operation while the switch is offline.

**Description** This operation cannot take place while the director or switch is offline.

**Action** Set the director or switch offline through the *Set Online State* dialog box and retry the operation.

**Message** Cannot remove all slot assignments from Partition 0.

**Description** The user has attempted to remove all slots from Partition 0, which would leave the partition disabled. The director firmware requires that Partition 0 be enabled.

**Action** Do not attempt to remove slots from Partition 0.

**Message** Cannot retrieve current SNMP configuration.

**Description** SNMP configuration information cannot be retrieved. The link is down or busy.

**Action** Retry the operation later. If the condition persists, contact support personnel and report the problem.

**Message** Cannot retrieve diagnostics results.

**Description** Diagnostics results cannot be retrieved. The link is down or busy.

**Action** Retry the operation later. If the condition persists, contact support personnel and report the problem.

<b>Message</b>	<b>Cannot retrieve port configuration.</b>
<b>Description</b>	Port configuration cannot be retrieved. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot retrieve port information.</b>
<b>Description</b>	Port information cannot be retrieved. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot retrieve port statistics.</b>
<b>Description</b>	Port statistics cannot be retrieved. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot retrieve switch date and time.</b>
<b>Description</b>	The director or switch date and time cannot be retrieved. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot retrieve switch state.</b>
<b>Description</b>	The director or switch state cannot be retrieved. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.

<b>Message</b>	<b>Cannot run diagnostics. The port card is not installed.</b>
<b>Description</b>	Port diagnostics cannot be performed when the port card is not installed.
<b>Action</b>	Run diagnostics only on a port that is installed.
<b>Message</b>	<b>Cannot run diagnostics on a port that is failed.</b>
<b>Description</b>	Port diagnostics cannot be performed on a port that has failed.
<b>Action</b>	Run port diagnostics only on an operational port.
<b>Message</b>	<b>Cannot run diagnostics on an active E-port.</b>
<b>Description</b>	Port diagnostics cannot be performed on a configured and active expansion port (E_Port).
<b>Action</b>	Run diagnostics only on an inactive E-port.
<b>Message</b>	<b>Cannot run diagnostics while a device is logged-in to the port.</b>
<b>Description</b>	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.
<b>Action</b>	Log out the device and run the diagnostic test again.
<b>Message</b>	<b>Cannot save IPL configuration file while active=save is enabled.</b>
<b>Description</b>	The user cannot save the IPL file while the active=save property is set.
<b>Action</b>	The FICON management server property, active=save, must be disabled for EFCM to save the IPL file.
<b>Message</b>	<b>Cannot save port configuration.</b>
<b>Description</b>	Port configuration cannot be saved. The link is down or busy.

**Action** Retry the operation later. If the condition persists, contact support personnel and report the problem.

**Message** Cannot save SNMP configuration.

**Description** SNMP configuration cannot be saved. The link is down or busy.

**Action** Retry the operation later. If the condition persists, contact support personnel and report the problem.

**Message:** Cannot set all ports to 1 Gb/sec due to port speed restriction on some ports.

**Description:** Displays if all ports are set to 1 Gb/sec through the *Configure Ports* dialog box and some ports do not support speed configuration.

**Action:** Replace ports that do not support speed configuration (FPM cards) with those that support more than one speed configuration (UPM cards).

**Message:** Cannot set all ports to 2Gb/sec due to port speed restriction on some ports.

**Description:** Displays if all ports are set to 2 Gb/sec through the *Configure Ports* dialog box and some ports do not support speed configuration.

**Action:** Replace ports that do not support speed configuration (FPM cards) with those that support more than one speed configuration (UPM cards).

**Message:** Cannot set all ports to Negotiate due to port speed restriction on some ports.

**Description:** Displays if all ports are set to *Negotiate* through the *Configure Ports* dialog box and some ports do not support speed configuration.

**Action:** Replace ports that do not support speed configuration (FPM cards) with those that support more than one speed configuration (UPM cards).

<b>Message</b>	<b>Cannot set Fibre Channel parameters.</b>
<b>Description</b>	Fibre Channel parameters cannot be set. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot set switch date and time.</b>
<b>Description</b>	The director or switch date and time cannot be set. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot set switch state.</b>
<b>Description</b>	The director or switch state cannot be set. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot set write authorization without defining a community name.</b>
<b>Description</b>	A community name was not defined in the <i>Configure SNMP</i> dialog box for the write authorization selected.
<b>Action</b>	Enter a community name in the name field where write authorization is checked.
<b>Message</b>	<b>Cannot start data collection.</b>
<b>Description</b>	Data collection cannot be started. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.



<b>Message</b>	<b>Cannot start firmware install while CTP synchronization is in progress.</b>
<b>Description</b>	CTP synchronization is in progress while the user is attempting to install firmware.
<b>Action</b>	Wait for the CTP synchronization to complete before starting the firmware install.
<b>Message</b>	<b>Cannot start port diagnostics.</b>
<b>Description</b>	Port diagnostics cannot be started. The link is down or busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Cannot swap an uninstalled port.</b>
<b>Description</b>	A port swap cannot be performed when the port card is not installed.
<b>Action</b>	Perform a swap only on a port that is installed.
<b>Message</b>	<b>Click OK to remove all contents from log.</b>
<b>Description</b>	Requesting confirmation to delete all contents from the selected log.
<b>Action</b>	Click <i>OK</i> to continue or <i>Cancel</i> to cancel the operation.
<b>Message</b>	<b>Connection to management server lost. Click OK to exit application.</b>
<b>Description</b>	The SAN management application at a remote workstation lost the network connection to the management server.
<b>Action</b>	Re-start the SAN management application to connect to the management server.

<b>Message</b>	<b>Continuing may overwrite host programming. Continue?</b>
<b>Description</b>	Configurations sent from the host may be overwritten by SAN management application.
<b>Action</b>	Continuing activates the current configuration and overwrites the host configuration.
<b>Message</b>	<b>Could not export log to file.</b>
<b>Description</b>	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.
<b>Action</b>	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
<b>Message</b>	<b>Could not find firmware file.</b>
<b>Description</b>	Firmware file selected was not found in the file transfer protocol (FTP) directory.
<b>Action</b>	Ensure the file name and directory are correct and retry the operation.
<b>Message</b>	<b>Could not remove dump files from server.</b>
<b>Description</b>	Dump files could not be removed from the server. The link may be down, or the director or switch may be busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Could not stop port diagnostics.</b>
<b>Description</b>	Port diagnostics could not be stopped. The link May be down or the director may be busy.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel.

<b>Message</b>	<b>Could not write firmware to flash.</b>
<b>Description</b>	Firmware could not be written to FLASH memory.
<b>Action</b>	Try again. If problem persists, contact support personnel.
<b>Message</b>	<b>CUP name and port name are identical.</b>
<b>Description</b>	Within the address configuration, one or more of the port names are the same as the CUP name.
<b>Action</b>	Make sure all names are unique for the ports and CUP name.

---

**D**

<b>Message</b>	<b>Date entered is invalid.</b>
<b>Description</b>	Date is entered incorrectly.
<b>Action</b>	Verify the number of days in the month entry is valid.
<b>Message</b>	<b>Device applications should be terminated before starting diagnostics. Press NEXT to continue.</b>
<b>Description</b>	Device application is not terminated.
<b>Action</b>	Terminate device application before running port diagnostics.
<b>Message</b>	<b>[device WWN] cannot be removed from the switch membership list while participating in switch binding. The device must be isolated from the switch, or switch binding deactivated before it can be removed.</b>
<b>Description</b>	A user attempted to remove a device WWN from the director or switch membership list (SANtegrity binding feature) with switch binding enabled.
<b>Action</b>	Disconnect the device by blocking the director or switch port and setting the director or switch offline, or disable switch binding through the <i>Switch Binding Change State</i> dialog box before removing devices from the membership list.

<b>Message</b>	<b>Director clock alert mode must be cleared before enabling period synchronization.</b>
<b>Description</b>	Clock alert mode is enabled through the <i>Configure FICON Management Server</i> dialog box and user is attempting to enable <i>Periodic Date/Time Synchronization</i> through the <i>Configure Date and Time</i> dialog box.
<b>Action</b>	Disable clock alert mode through the <i>Configure FICON Management Server</i> dialog box.
<b>Message</b>	<b>Disabling Insistent Domain ID will disable fabric binding. Do you want to continue?</b>
<b>Description</b>	Fabric binding is enabled through the SAN management application and a user attempted to disable the <i>Insistent Domain ID</i> parameter at the <i>Configure Switch Parameters</i> dialog box.
<b>Action</b>	Click <i>Yes</i> to continue and disable fabric binding.
<b>Message</b>	<b>Disabling switch binding will disable Enterprise Fabric Mode. Do you want to continue?</b>
<b>Description</b>	A user attempting to disable switch binding through the <i>Switch Binding State Change</i> dialog box, but <i>Enterprise Fabric Mode</i> is enabled.
<b>Action</b>	Disable <i>Enterprise Fabric Mode</i> at the <i>Enterprise Fabric Mode</i> dialog box before disabling switch binding.
<b>Message</b>	<b>Do you want to continue with IPL?</b>
<b>Description</b>	Message requesting confirmation to proceed with an IPL.
<b>Action</b>	Click <i>Yes</i> to confirm the IPL or <i>Cancel</i> to cancel the operation.
<b>Message</b>	<b>Duplicate community names require identical write authorizations.</b>
<b>Description</b>	Duplicate community names exist that have conflicting or different write authorizations.

**Action** Verify community names and whether a community name is duplicated with different write authorizations.

**Message** Duplicate port names detected.

**Description** Ports cannot have the same name.

**Action** Rename ports using the *Configure Ports* option in the *Configure* menu.

---

## E

**Message** Exclusive management server connection to the director required for this command.

**Description** You attempted to execute a command that is not valid when more than one management server is connected to the director.

**Action** Exit the additional management servers so that only one is connected to the director.

**Message** Element Manager error <number>.

**Description** The Element Manager application encountered an internal error and cannot continue.

**Action** Contact support personnel and report the problem.

**Message** Element Manager instance is currently open.

**Description** An instance of the Element Manager application is already open.

**Action** Information message - no action required.

**Message** Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCN's. Do you want to continue?

<b>Description</b>	The user attempted to disable one or more of these parameters at the <i>Configure Switch Parameters</i> dialog box with the director or switch online and <i>Enterprise Fabric Mode</i> (SANtegrity binding feature) enabled.
<b>Action</b>	Click <i>Yes</i> to continue and disable <i>Enterprise Fabric Mode</i> .
<b>Message</b>	<b>Error retrieving port information.</b>
<b>Description</b>	An error occurred while retrieving port information. The link is down or busy.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Error retrieving port statistics.</b>
<b>Description</b>	An error occurred while retrieving port statistics. The link is down or busy.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Error stopping port diagnostics.</b>
<b>Description</b>	An error occurred while attempting to stop the port diagnostics from running. The link is down or busy.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Error transferring files &lt; message &gt;.</b>
<b>Description</b>	An error occurred while transferring files from the PC hard drive to the Element Manager application. The message varies, depending on the problem.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.

---

**F**

<b>Message</b>	<b>Feature not supported. The Product Name must be running version 05.00.00 or higher.</b>
<b>Description</b>	The Enterprise Operating System (E/OS) version running on the director or switch is lower than Version 05.00.00. This message displays only if the optional OpenTrunking feature is installed.
<b>Action</b>	Install E/OS Version 5.00.00 or higher.
<b>Message</b>	<b>Field cannot be blank.</b>
<b>Description</b>	Data field requires an entry and cannot be left blank.
<b>Action</b>	Enter appropriate information in the data field.
<b>Message</b>	<b>Field has exceeded maximum number of characters.</b>
<b>Description</b>	Maximum number of characters allowed in a data entry field was exceeded.
<b>Action</b>	Enter information using the allowed number of characters.
<b>Message</b>	<b>File transfer aborted.</b>
<b>Description</b>	User has stopped the file transfer.
<b>Action</b>	Verify the file transfer is to be aborted, then click <i>OK</i> to continue.
<b>Message</b>	<b>File transfer is in progress.</b>
<b>Description</b>	Firmware or data collection information is being transferred.
<b>Action</b>	Information message - no action required.

**Message**      **Firmware download timed out.**

**Description**      The director or switch did not respond in the time allowed, causing the firmware download to time out.

**Action**      Retry the operation. If the condition persists, contact support personnel and report the problem.

**Message**      **Firmware file I/O error.**

**Description**      Firmware file I/O error occurred.

**Action**      Retry the operation. If the condition persists, contact support personnel and report the problem.

**Message**      **Firmware file not found.**

**Description**      Firmware file was deleted from management server.

**Action**      Add the firmware version to the library.

---

I

**Message**      **Incompatible configuration between operating mode and management server.**

**Description**      The user has selected the open systems operating mode, but has the FICON Management Server feature installed, and is attempting to activate the operating mode.

**Action**      User needs to install Open Systems Management Server or select the FICON operating mode.

**Message**      **Incorrect product type.**

**Description**      When configuring a new product through the *New Product* dialog box, an incorrect product was selected for the network address.

**Action**      Select the correct product type for the product with the network address.



<b>Message</b>	<b>Installing this feature key while online will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?</b>
<b>Description</b>	If the director or switch is online, installing a feature key causes a director or switch IPL. The LAN connection to the management server is lost momentarily, but Fibre Channel traffic is not affected.
<b>Action</b>	Click <i>Yes</i> to install the feature key or <i>No</i> to discontinue the operation.
<b>Message</b>	<b>Internal file transfer error received from switch.</b>
<b>Description</b>	Director or switch detected an internal file transfer error.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Invalid character in field.</b>
<b>Description</b>	Invalid character in the input field.
<b>Action</b>	Remove invalid characters from the entry.
<b>Message</b>	<b>Invalid configuration name.</b>
<b>Description</b>	The user attempted to save an invalid address configuration name.
<b>Action</b>	Enter a configuration name of up to 24 alphanumeric characters, including spaces, hyphens and underscores.
<b>Message</b>	<b>Invalid feature key.</b>
<b>Description</b>	The entered feature key was not recognized.
<b>Action</b>	Re-enter the feature key. The key is case sensitive and includes dashes.

<b>Message</b>	<b>Invalid firmware file.</b>
<b>Description</b>	Selected file is not a valid firmware file.
<b>Action</b>	Select the correct firmware file and retry the operation.
<b>Message</b>	<b>Invalid management server address.</b>
<b>Description</b>	The IP address specified for the management server is unknown to the domain name server (invalid).
<b>Action</b>	Verify and enter a valid management server IP address.
<b>Message</b>	<b>Invalid network address.</b>
<b>Description</b>	Network address specified is not known by the domain name server.
<b>Action</b>	Check the input address and specify the correct network address.
<b>Message</b>	<b>Invalid port address.</b>
<b>Description</b>	Invalid port address has been entered.
<b>Action</b>	Verify port address through the <i>Configure Addresses - "Active"</i> dialog box and re-enter.
<b>Message</b>	<b>Invalid port number. Valid ports are (0-&lt; nn &gt;).</b>
<b>Description</b>	The user has specified an invalid port number.
<b>Action</b>	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus one. For example, for a director with 64 ports, the valid port range is 0 to 139.

<b>Message</b>	<b>Invalid port swap.</b>
<b>Description</b>	Port swap selection is not allowed.
<b>Action</b>	Ensure that each port selected for swap has not been previously swapped.
<b>Message</b>	<b>Invalid response received from switch.</b>
<b>Description</b>	An error occurred and the director or switch returned an invalid response.
<b>Action</b>	Resend the firmware. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Invalid serial number for this feature key.</b>
<b>Description</b>	The director or switch serial number and the entered feature key do not match.
<b>Action</b>	Ensure that the entered feature key corresponds to the director or switch serial number.
<b>Message</b>	<b>Invalid UDP port number.</b>
<b>Description</b>	The user datagram protocol (UDP) port number must be an integer from 1 through 65535.
<b>Action</b>	Enter a port number from 1 through 65535.
<b>Message</b>	<b>Invalid value for BB_Credit.</b>
<b>Description</b>	<i>BB_Credit</i> must be an integer from 1 through 60.
<b>Action</b>	Enter a BB_Credit value from 1 through 60.

<b>Message</b>	<b>Invalid value for Low BB Credit threshold (1-99) %.</b>
<b>Description</b>	<i>Low BB Credit Threshold</i> text field in <i>Configure Open Trunking</i> dialog box must have entries in the range from 1 and 99. This message only displays if the optional Open Trunking feature is installed. Note that your message and the <i>Configure Open Trunking</i> dialog box may display <i>Credit Starvation Threshold</i> instead of <i>Low BB Credit Threshold</i> .
<b>Action</b>	Enter a value from 1 to 99 into the <i>Low BB Credit Threshold</i> of the <i>Configure Open Trunking</i> dialog box.
<b>Message</b>	<b>Invalid value for day (1 - 31).</b>
<b>Description</b>	Value for <i>Day</i> must be an integer from 1 through 31.
<b>Action</b>	Enter a value from 1 through 31.
<b>Message</b>	<b>Invalid value for E_D_TOV.</b>
<b>Description</b>	Value for <i>E_D_TOV</i> must be an integer from 2 through 600 milliseconds.
<b>Action</b>	Enter a value from 2 through 600.
<b>Message</b>	<b>Invalid value for hour (0 - 23).</b>
<b>Description</b>	Value for <i>Hour</i> must be an integer from 0 through 23.
<b>Action</b>	Enter a value from 0 through 23.
<b>Message</b>	<b>Invalid value for Low BB_Credit Threshold (1 - 99%).</b>
<b>Description</b>	The <i>Low BB_Credit Threshold</i> value at the <i>Configure OpenTrunking</i> dialog box must be an integer from 1 through 99. This message displays only if the optional OpenTrunking feature is installed.
<b>Action</b>	At the <i>Configure OpenTrunking</i> dialog box, enter a <i>Low BB_Credit Threshold</i> value from 1 through 99 percent.

<b>Message</b>	<b>Invalid value for minute (0 - 59).</b>
<b>Description</b>	Value for <i>Minute</i> must be an integer from 0 through 59.
<b>Action</b>	Enter a value from 0 through 59.
<b>Message</b>	<b>Invalid value for month (1 - 12).</b>
<b>Description</b>	Value for <i>Month</i> must be an integer from 1 through 12.
<b>Action</b>	Enter a value from 1 through 12.
<b>Message</b>	<b>Invalid value for R_A_TOV.</b>
<b>Description</b>	Value for <i>R_A_TOV</i> must be an integer from 10 through 1200.
<b>Action</b>	Enter a value from 10 to 1200.
<b>Message</b>	<b>Invalid value for second (0 - 59).</b>
<b>Description</b>	Value for <i>Second</i> must be an integer from 0 through 59.
<b>Action</b>	Enter a value from 0 through 59.
<b>Message</b>	<b>Invalid value for Threshold (1 - 99%).</b>
<b>Description</b>	The <i>Threshold %</i> value for each configured Fibre Channel port at the <i>Configure OpenTrunking</i> dialog box must be an integer from 1 through 99. This message displays only if the optional OpenTrunking feature is installed.
<b>Action</b>	At the <i>Configure OpenTrunking</i> dialog box, enter a <i>Threshold %</i> value for each configured port from 1 through 99 percent.
<b>Message</b>	<b>Invalid value for year.</b>
<b>Description</b>	Value for <i>Year</i> must be a four-digit value and after 1980.
<b>Action</b>	Enter a four-digit value for the year.

**Message** Invalid World Wide Name.

**Description** The WWN must have eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).

**Action** Enter a WWN using eight two-digit hexadecimal numbers separated by colons.

---

**L**

**Message** Link dropped.

**Description** The director (or switch)-to-management server link was dropped.

**Action** Wait approximately 30 seconds for the link to establish and retry the operation. If the condition persists, contact support personnel.

**Message** Log is currently in use.

**Description** The selected log is in use by another Element Manager instance.

**Action** Retry the operation. If the condition persists, contact support personnel and report the problem.

**Message** Loopback plug(s) must be installed on ports being diagnosed. Press NEXT to continue.

**Description** An optical loopback plug must be installed in a Fibre Channel port prior to performing an external loopback diagnostic test.

**Action** Ensure an optical loopback plug is installed in the port, then restart the test.

---

**M**

**Message** Maximum number of versions already installed.

**Description** The maximum number of firmware versions has been reached.

**Action** Delete a firmware version before adding a new firmware version.

**Message** **McDATA SANtegrity binding feature not installed. Please contact your sales representative.**

**Description** A user selected *Switch Binding* from the *Configure* menu. This selection is not supported because the SANtegrity binding feature is not installed.

**Action** Install the optional SANtegrity binding feature key through the *Configure Feature Key* dialog box before enabling switch binding.

## N

**Message** **Nickname already exists. Please use a different nickname.**

**Description** The entered nickname already exists.

**Action** Specify a unique nickname.

**Message** **No backup configuration available to restore.**

**Description** A backup of the configuration is not on the management server hard drive. A configuration restore cannot be completed.

**Action** Select *Backup and Restore Configuration* from the *Maintenance Menu* and select *Backup* to create a backup configuration file.

**Message** **No file was selected.**

**Description** A required file was not selected before an action was performed.

**Action** Select the required file and retry the operation.

**Message** **No firmware version file was selected.**

**Description** A firmware file was not selected in the *Firmware Library* dialog box before an action was performed.

**Action** Select a firmware version and perform the action again.

<b>Message</b>	<b>No firmware versions to delete.</b>
<b>Description</b>	There are no firmware versions in the firmware library to delete.
<b>Action</b>	Information message - no action required.
<b>Message</b>	<b>No firmware versions was selected.</b>
<b>Description</b>	A file was not selected in the <i>Firmware Library</i> dialog box before an action, such as <i>modify</i> or <i>send</i> was performed.
<b>Action</b>	Click on a firmware version in the dialog box to select it, then perform the action again.
<b>Message</b>	<b>Non-redundant switch must be offline to install firmware.</b>
<b>Description</b>	If the director has only a single CTP card, it must be offline to initiate a firmware installation. (Switches have only one CTP card.)
<b>Action</b>	Set director or switch offline and try the firmware installation again.
<b>Message</b>	<b>Not all of the optical transceivers are installed for this range of ports.</b>
<b>Description</b>	One or more ports in the specified port range do not have optical transceivers installed.
<b>Action</b>	Specify a port range valid for ports installed.

---

**P**

<b>Message</b>	<b>Performing this operation will change the current state to offline.</b>
<b>Description</b>	This operation causes the director or switch to go offline.
<b>Action</b>	Information message - no action required.



<b>Message</b>	<b>Performing this operation will change the current state to online.</b>
<b>Description</b>	This operation causes the director or switch to go online.
<b>Action</b>	Information message - no action required.
<b>Message</b>	<b>Performing this action will overwrite the date/time on the switch.</b>
<b>Description</b>	This warning message occurs when entering parameters through the <i>Configure Date and Time</i> dialog box, and indicates the new date and time will overwrite the existing date and time or set for the director or switch.
<b>Action</b>	Verify that you want to overwrite the current date or time.
<b>Message</b>	<b>Periodic Date/Time synchronization must be cleared before enabling director clock alert.</b>
<b>Description</b>	This action cannot be performed because the <i>Periodic Date/Time Synchronization</i> option is enabled.
<b>Action</b>	Click the <i>Periodic Date/Time Synchronization</i> check box at the <i>Configure Date and Time</i> dialog box to clear check mark and disable the periodic date and time synchronization option.
<b>Message</b>	<b>Port binding was removed from attached devices that are also participating in switch binding.</b>
<b>Description</b>	A user disabled port binding for attached devices, but one or more of the devices is controlled by fabric binding.
<b>Action</b>	Review the switch binding membership list to determine if devices should or should not be included.
<b>Message</b>	<b>Port cannot swap to itself.</b>
<b>Description</b>	Port addresses entered in the <i>Swap Ports</i> dialog box are the same.
<b>Action</b>	Ensure that address in the first and second port address fields are different.

**Message:** Port diagnostics cannot be performed on an inactive port.

**Description:** Displays when port diagnostics is run on a port that in an inactive state.

**Action:** Perform diagnostics on an active port.

**Message:** Port speeds cannot be configured at a higher rate than the switch speed.

**Description:** An attempt was made to configure a port to 2.125 Gbps with the director or switch speed set to 1.0625 Gbps.

**Action:** Set the director speed to 2 Gb/sec in the *Configure Operating Parameter* dialog box.

**Message** Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters.

**Description** If the switch's domain ID has not been set to *Insistent*, the user is not allowed to activate the Preferred Path configuration with the *Enable Preferred Paths* check box selected.

**Action** Close the *Configure Preferred Paths* dialog box and select the *Configure* menu, then *Operating Parameters*, then *Switch Parameters*. On the *Configure Switch Parameters* dialog box, select the *Insistent* check box.

---

## R

**Message** R\_A\_TOV must be greater than E\_D\_TOV.

**Description** R\_A\_TOV value must be greater than E\_D\_TOV value.

**Action** Change a value so R\_A\_TOV exceeds E\_D\_TOV.

<b>Message</b>	<b>Resource is unavailable.</b>
<b>Description</b>	The specified operation cannot be performed because the product is unavailable.
<b>Action</b>	Verify the director (or switch)-to-management server link is operational. If the link is up, the management server may be busy. Try the operation later.

---

**S**

<b>Message</b>	<b>Send firmware failed.</b>
<b>Description</b>	Send firmware operation failed.
<b>Action</b>	Retry the operation. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>SNMP trap address not defined.</b>
<b>Description</b>	An SNMP trap address must be defined if a community name is defined.
<b>Action</b>	Define an SNMP address.
<b>Message</b>	<b>Stop diagnostics failed. The test is already running.</b>
<b>Description</b>	Diagnostics for the port were not running and <i>Stop</i> was selected at the <i>Port Diagnostics</i> dialog box. Diagnostics aborted for some reason, but the <i>Stop</i> button remains enabled.
<b>Action</b>	Verify port operation. Retry diagnostics for the port and select <i>Stop</i> from the dialog box. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>Stop diagnostics failed. The test was not running.</b>
<b>Description</b>	The action to stop diagnostics failed because the test was not running.
<b>Action</b>	Information message - no action required.

**Message** Switch binding was removed from attached devices that are also participating in port binding. Please review the port binding configuration.

**Description** Device WWNs were removed from the switch membership list (SANtegrity binding feature), but one or more of the devices still has security controlled by port binding.

**Action** Verify the security level for each device is specified as required by reviewing the *Bound WWN* list at the *Configure Ports* dialog box.

**Message** System diagnostics cannot run. The operational status is invalid.

**Description** System diagnostics cannot run on a director or switch with failed ports.

**Action** Replace failed ports.

---

**T**

**Message** The add firmware process has been aborted.

**Description** User has ended the add firmware process.

**Action** Information message - no action required.

**Message** The data collection process failed.

**Description** An error occurred in the data collection procedure.

**Action** Contact support personnel and report the problem.

**Message** The data collection process has been aborted.

**Description** User has ended the data collection process.

**Action** Information message - no action required.

<b>Message</b>	<b>The default zone must be disabled to configure.</b>
<b>Description</b>	A user attempted to change the switch interoperability mode to <i>Open Fabric Mode</i> with the default zone enabled.
<b>Action</b>	Disable the default zone and repeat the operation.
<b>Message</b>	<b>The management server is busy processing a request from another Element Manager.</b>
<b>Description</b>	The management server could not process the current request because it is busy handling a request from another Element Manager.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>The Ethernet link dropped.</b>
<b>Description</b>	The Ethernet connection between the management server and the director or switch is down or unavailable.
<b>Action</b>	Establish and verify the network connection.
<b>Message</b>	<b>The firmware file is corrupted.</b>
<b>Description</b>	A firmware version file is corrupt.
<b>Action</b>	Contact support personnel and report the problem.
<b>Message</b>	<b>The firmware version already exists.</b>
<b>Description</b>	This firmware version already exists in the database.
<b>Action</b>	Information message - no action required.

<b>Message</b>	<b>The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCN's.</b>
<b>Description</b>	A user attempted to disable one or more of these parameters at the <i>Configure Switch Parameters</i> dialog box with the director or switch online and <i>Enterprise Fabric Mode</i> (SANtegrity binding feature) enabled.
<b>Action</b>	Click <i>Yes</i> to continue and disable <i>Enterprise Fabric Mode</i> .
<b>Message</b>	<b>The IPL configuration cannot be deleted.</b>
<b>Description</b>	A user attempted to delete the IPL address configuration. This operation is not allowed.
<b>Action</b>	Cancel the operation.
<b>Message</b>	<b>The link to the switch is not available.</b>
<b>Description</b>	The Ethernet director (or switch)-to-management server link is not available.
<b>Action</b>	Check the Ethernet connection. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>The maximum number of address configurations has been reached.</b>
<b>Description</b>	The maximum number of address configurations that can be saved to the management server was reached.
<b>Action</b>	Delete configurations no longer needed to allow one or more new address configurations to be saved.
<b>Message</b>	<b>The optical transceiver is not installed.</b>
<b>Description</b>	Information is not available for a port without an optical transceiver installed.
<b>Action</b>	Install an SFP optical transceiver in the port.

<b>Message</b>	<b>The switch did not accept the request.</b>
<b>Description</b>	The director or switch was not able to perform the requested action.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>The switch did not respond in the time allowed.</b>
<b>Description</b>	The director or switch did not respond in the time allowed, causing a time out.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>The switch is busy saving maintenance information.</b>
<b>Description</b>	The director or switch is busy performing a maintenance operation.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.
<b>Message</b>	<b>The switch must be offline to configure.</b>
<b>Description</b>	A configuration change was attempted that requires the director or switch to be set offline.
<b>Action</b>	Set the director or switch offline and retry the configuration change.
<b>Message</b>	<b>This feature has not been installed. Please contact your sales representative.</b>
<b>Description</b>	A user selected an option that is unavailable because a necessary feature is not installed.
<b>Action</b>	Contact your sales representative to obtain and install the desired optional feature.

**Message** This feature key does not include all of the features currently installed and cannot be activated while the switch is online.

**Description** The installed feature set contains features not being installed with the new feature key. To activate the new feature key, you must set the director or switch offline. Activating the new feature set removes features not in the new feature set.

**Action** Set the director or switch offline through the *Set Online State* dialog box. Activate the new feature key using the *Configure Feature Key* dialog box.

**Message** This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?

**Description** The installed feature set contains features not being installed with the new feature key.

**Action** Click *Yes* to activate the feature key and remove current features not in the new feature set or *No* to cancel the operation.

**Message** Threshold alerts are not supported on firmware earlier than 01.03.00.

**Description** Threshold alerts are not supported for firmware versions released prior to Version 1.03.00.

**Action** Information message - no action required.

---

## U

**Message** Unable to change to incompatible firmware release.

**Description** The firmware you are trying to download cannot be used for this Element Manager application release.

**Action** Download compatible firmware for this Element Manager application release.



<b>Message</b>	Unable to save data collection file to destination.
<b>Description</b>	Could not save data collection file to the specified drive.
<b>Action</b>	Retry the operation later. If the condition persists, contact support personnel and report the problem.

---

**Y**

<b>Message</b>	You do not have rights to perform this action.
<b>Description</b>	User does not have the rights to perform this action.
<b>Action</b>	Information message - no action required.



## Event Code Tables

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a director operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Events are reported as event codes.

This appendix lists the three-digit event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format, and are grouped as follows:

- 000 through 199 - System events.
- 200 through 299 - Power supply events.
- 300 through 399 - Fan module events.
- 400 through 499 - Control processor (CTP) card events.
- 500 through 599 - Port card (UPM and XPM) events.
- 600 through 699 - Serial crossbar (SBAR) events.
- 800 through 899 - Thermal events.

Events are recorded in the Intrepid 6140 *Event Log*, in the event log of the Web server, at a remote workstation if E-mail and call-home features are enabled, or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error light-emitting diode (LED) on the director front bezel.

In addition to numerical event codes, the tables in this appendix also provide a:

- **Message** - A brief text string that describes the event.
- **Severity** - A severity level that indicates event criticality as follows:
  - Informational.
  - Minor.
  - Major.
  - Severe (not operational).
- **Explanation** - An explanation of what caused the event.
- **Action** - The recommended course of action (if any) to resolve the problem.
- **Event data** - Supplementary event data (if any) that appears in the event log in hexadecimal format.
- **Distribution** - Check marks in associated fields indicate where the event code is reported (director, management server, or host).

## System Events (000 through 199)

Event Code: 001							
Message:	System power-down.						
Severity:	Informational.						
Explanation:	The director was powered off or disconnected from the facility AC power source. The event code is distributed the next time the director powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 010							
Message:	Login Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Login Server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. All fabric services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 011**

Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP card failover or replacement, initial machine load (IML), or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All fabric services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 020**

Message:	Name Server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the Name Server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. All fabric services databases are initialized to an empty state, resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 021**

Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP card failover or replacement, IML, or firmware download, the Name Server database failed its CRC validation. All fabric services databases are initialized to an empty, state resulting in an implicit fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 031**

Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the management server application are allowed.						
Action:	Add the community name to the SNMP configuration using the management server application.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 050**

Message:	Management server unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the management server attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. All management services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the management server.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 051**

Message:	Management server database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP card failover or replacement, IML, or firmware download, the management server database failed its CRC validation. All management services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the management server.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		



Event Code: 052							
Message:	Management server internal error.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the management server application.						
Action:	Management server application internal error: Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Supplementary data consists of reporting tasks of type <b>eMST_SB2</b> , with component_id <b>eMSCID_SB2_CHPGM</b> . For each type of error or indication, the subcomponent_id is: Management server internal error: subcomponent_id is <b>eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR</b> or <b>eMS_ELR_SB2_MSG_PROCESSING_ERROR</b> .						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

Event Code: 060							
Message:	Fabric controller unable to synchronize databases.						
Severity:	Minor.						
Explanation:	Following a CTP card reset or replacement, the fabric controller attempted to acquire an up-to-date copy of its databases from the other CTP card, but failed. All fabric controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 061**

Message:	Fabric controller database invalid.						
Severity:	Minor.						
Explanation:	Following a CTP card failover or replacement, IML, or firmware download, the fabric controller database failed its CRC validation. All fabric controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 062**

Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (director or switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two directors or switches traverses no more than seven ISLs.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) more than seven hops away. Bytes 1 - 3 = reserved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The fabric element (director or switch) whose domain ID is indicated in the event data has too many ISLs attached, and that element is unreachable from this director. Element Manager application Version 3.2 and earlier supports up to 32 ISLs. Element Manager application Version 3.3 and later supports up to 128 ISLs.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) with too many ISLs. Bytes 1 - 3 = reserved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓			

Event Code: 064							
Message:	ESS response from indicated domain not received after maximum tries exhausted.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that the ESS response from the indicated domain has not been received after the maximum number of attempts. Event posts in McDATA interop mode only.						
Action:	No action required.						
Event Data:	Byte 0 = domain ID of the fabric element (director or switch) not receiving a response to an ESS message. Byte 1 = domain ID of the fabric element (director or switch) not responding. Bytes 2- 3 = reserved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 070	
Message:	E_Port is segmented.
Severity:	Informational.
Explanation:	A director E_Port recognized an incompatibility with an attached fabric element (director or switch), preventing the director from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached director or switch). See the event data below for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the E_Port number. The fifth byte (byte <b>4</b>) specifies the segmentation reason as follows:</p> <p><b>1 = Incompatible operating parameters.</b> Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the director and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p><b>2 = Duplicate domain ID.</b> The director has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p><b>3 = Incompatible zoning configurations.</b> The same name is applied to a zone for the director and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p><b>4 = Build fabric protocol error.</b> A protocol error was detected during incorporation of the director into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p><b>5 = No principal switch.</b> No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p><b>6 = No response from attached switch (hello timeout).</b> The director periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the CD to McDATA support personnel.</p>

**Event Code: 070 (continued)**

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓	✓			

**Event Code: 071**

Message:	Switch is isolated.
Severity:	Informational.
Explanation:	The director is isolated from other fabric elements (directors or switches). This event code is accompanied by one or more <b>070</b> event codes. Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the E_Port number. The fifth byte (byte <b>4</b>) specifies the segmentation reason as follows:</p> <p><b>1 = Incompatible operating parameters.</b> Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the director and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p><b>2 = Duplicate domain ID.</b> The director has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p><b>3 = Incompatible zoning configurations.</b> The same name is applied to a zone for the director and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p><b>4 = Build fabric protocol error.</b> A protocol error was detected during incorporation of the director into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p><b>5 = No principal switch.</b> No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p><b>6 = No response from attached switch (hello timeout).</b> The director periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the CD to McDATA support personnel.</p>

## Event Code Tables

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 072**

Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The director is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte 0 = error reason code for engineering evaluation. Bytes 4 - 9 = port numbers for which problems were detected.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (073 event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte 0 = E_Port number reporting the problem. Bytes 4 - 7 = Count of frame delivery timeouts. Bytes 8- 11 = Count of frame delivery aborts.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 075							
Message:	E_Port segmentation recovery.						
Severity:	Informational.						
Explanation:	A segmented E_Port has recovered. Event is not generated if port is manually recovered by blocking/unblocking, offline/online, or removing/inserting ISL. See the event data below for the segmentation reason.						
Action:	Informational (see event <b>070</b> ).						
Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the E_Port number. The fifth byte (byte <b>4</b>) specifies the segmentation reason as follows:</p> <p><b>1 = Incompatible operating parameters.</b> Either the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the director and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.</p> <p><b>2 = Duplicate domain ID.</b> The director has the same preferred domain ID as another fabric element (director or switch). Modify the director's Domain ID to make it unique.</p> <p><b>3 = Incompatible zoning configurations.</b> The same name is applied to a zone for the director and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.</p> <p><b>4 = Build fabric protocol error.</b> A protocol error was detected during incorporation of the director into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the CD to McDATA support personnel.</p> <p><b>5 = No principal switch.</b> No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.</p> <p><b>6 = No response from attached switch (hello timeout).</b> The director periodically verifies operation of attached fabric elements (directors or switches). The director E_Port (at the operational director) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the CD to McDATA support personnel.</p>						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓	✓			



**Event Code: 080**

Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The worldwide name of the device or director plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or director into this port.						
Event Data:	Byte 0 = Port number reporting the unauthorized connection. Bytes 1 - 3 = reserved. Bytes 4 - 11 = WWN of the unauthorized device or fabric element.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓	✓		✓	

**Event Code: 081**

Message:	Invalid attachment.						
Severity:	Informational.						
Explanation:	A director port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.						
Action:	Action depends on the reason specified in the event data.						

Event Data:	<p>The first byte of event data (byte <b>0</b>) specifies the port number. The fifth byte (byte <b>4</b>) specifies the isolation reason as follows:</p> <p><b>1 = Unknown</b> - Isolation reason is unknown, but probably caused by failure of a device attached to the director through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem.</p> <p><b>2 = Non E_Port mode</b> - Port on this director or other side of ISL is set to F_Port only mode. Change mode of port to G_Port or E_Port.</p> <p><b>3 = Process ELP reject with unable to process reason code</b> - Indicates connection errors with non-McDATA switch. If connected to non-McDATA switch, contact the vendor.</p> <p><b>4 = Process ELP reject with invalid revision level</b> - Should only happen when connected to non-McDATA switch. Indicates it is not compatible with the revision level in ELP frame. Switches are not compatible.</p> <p><b>5 = Loopback indication</b> - Port is connected to another port on the same director or a loopback plug is inserted. Or two switches have the same WWN. REmove the loopback plug or ISL.</p> <p><b>6 = Non-F_Port mode</b> - Detect that a switch is attached to a port set to F_Port only mode. Change mode of port.</p> <p><b>7 = When in legacy mode detect connection over E_Port of a non-McDATA switch based on the WWN</b> - If wish to connect to non-McDATA switch, set switch mode to Open Fabric.</p> <p><b>8 = E_Port capability disabled and receive ELP</b> - Port configuration issue.</p> <p><b>A = Unauthorized port binding WWN</b> - Port binding security authorization on either F_Port or E_Port. Modify port binding WWN or disable port binding on the port.</p> <p><b>B = G_Port ELP timeout</b> - Unresponsive node connected to port. Timed out sending ELP frames and not get FLOGI or good response to sent ELP. Indicate problem with attached device. Can happen with connection to either switch or device. Check status of attached device.</p> <p><b>C = ESA security mismatch</b> - Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and director binding parameters for this director and the attached fabric element must agree. Ensure the parameters for both fabric elements are compatible or disable the fabric and director binding features.</p> <p><b>D = Fabric binding mismatch</b> - Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. Could also be the result of problems delivering EFMD ILS. Update the fabric membership list for both fabric elements to ensure compatibility or disable the fabric binding feature.</p> <p><b>E = Authorization failure reject</b> - The fabric element connected to the director through an ISL detected a security violation. As a result, the director received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors).</p> <p><b>F = Unauthorized switch binding WWN</b> - Director binding is enabled and an attached device or fabric element has an incompatible director membership list. Update the director membership list for the director and the attached device or fabric element to ensure compatibility or disable the director binding feature.</p> <p><b>10 = Authentication failure</b> - Authentication check (CHAP) failed. Update the authentication lists or disable authentication.</p> <p><b>11 = Fabric mode mismatch</b> - Based on the ELP revision level, a connection was not allowed because a McDATA switch in legacy mode is attached to a McDATA switch in Open Fabric mode, or a McDATA switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch.</p> <p><b>12 = CNT WAN extension mode mismatch</b> - Based on ELP maximum frame size, assume that connected to a switch in the CNT WAN extension mode. When in the CNT WAN extension mode, the maximum frame size is different. Update one of the switches to the correct WAN extension mode.</p>
-------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

**Event Code: 082**

Message:	Port fencing - port fenced.						
Severity:	Informational.						
Explanation:	Port is disabled (blocked) due to meeting the threshold criteria defined in the port fencing policy. The fence type is indicated in the event data.						
Action:	Identify the responsible application or hardware and fix. Hardware may include components such as ports, ISLs, and extenders. Port fencing threshold settings can be changed to lesser values. Unblock the port after problem has been fixed.						
Event Data:	<p>Bytes <b>0 - 3</b> = Port number.</p> <p>Bytes <b>4 - 7</b> = Fence type codes as follows:  <b>0 = None</b> - No type.  <b>1 = Protocol error</b> - This type of failure is associated with persistent application layer protocol error or persistent incomplete operations. This class would include perpetual port log-in, constant fabric rebuilds, and persistent in-band management protocol errors.  <b>2 = Link level hot I/O</b> - The family of failures is associated with hardware and an unstable link state machine.  <b>3 = Security violation</b> - The class of failures associated with persistent violations of one or more security features within E/OS (port binding violation, authentication failures, etc.).</p> <p>Bytes <b>8 - 11</b> = Disabled reason codes as follows:  <b>1 = Unknown</b> - Reason is not known.  <b>9 = ISL fencing</b> - ISL was fenced after meeting the threshold for port</p>						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓			✓	

**Event Code: 090**

Message:	Database replication time out.						
Severity:	Minor.						
Explanation:	Replication of a fabric services database from master CTP to backup CTP has timed out. The backup CTP has been dumped and IPLed. After the backup CTP completes the IPL, its databases will be brought up to date and replication will resume.						
Action:	Perform a data collection for this director using the SAN management application. Save the data file to the management server CD drive, and return the CD to McDATA support personnel.						
Event Data:	Bytes <b>0 - 3</b> : Type of replication operation that timed out.						
Distribution:	Director		Management Server			Host	
	SANpilot Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 091**

Message:	Database replication discontinued.						
Severity:	Informational.						
Explanation:	Replication of a fabric services database from master CTP to backup CTP has been discontinued because backup CTP has failed or been removed.						
Action:	This event will occur when the backup CTP fails or is removed, and does not require any additional action. When the backup CTP is recovered or replaced, its databases will be brought up to date and replication will resume. If this event occurs without the backup CTP failing or being removed, perform a data collection for this director using the SAN management application. Save the data file to the management server CD drive, and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives an SAN management command that violates specified boundary conditions, typically as a result of a network error. The director rejects the command, drops the director-to-management server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this director using the SAN management application. Save the data file to the management server CD drive, and return the CD to McDATA support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the director receives a zone set activation command that exceeds the size supported by the director. The director rejects the command, drops the director-to-management server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 140**

Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 141**

Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 142							
Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 143							
Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 150							
Message:	Zone merge failure.						
Severity:	Informational.						
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a <b>070</b> ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.						
Action:	Action depends on the failure reason specified in the event data.						
Event Data:	Bytes <b>0 - 3</b> of the event data specify affected E_Port number(s). Bytes <b>4 - 7</b> specify the request SW_ILS command code. Bytes <b>8 - 31</b> specify the request response payload.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓				

Event Code: 151							
Message:	Fabric configuration failure.						
Severity:	Informational.						
Explanation:	<p>A fabric-wide configuration activation failed. For example, a zone set activation.</p> <p>An event <b>151</b> is only logged by the managing switch. It is intended to detect and log errors that occur on the managing switch in the fabric when fabric configuration failures are detected. It is intended to help engineering personnel determine the cause of fabric-configuration failures.</p> <p>The event <b>151</b> is only possible in EOS versions 5.1 and above. All data values of the event are in big-endian notation, regardless of the embedded processor. All data values are hexadecimal and range from 0x00000000 and 0x000000FF.</p>						
Action:	Depends on the failure reason. In most cases, perform the data collection procedure on the managing switch and the managed switch, and return the CD to McDATA support personnel.						



Event Data:	<p>Reason codes were mapped from the software implementation (FC-SW2 protocol) so decoding them is complicated and may require engineering assistance.</p> <p>Bytes <b>0 - 3</b> = managing switches domain ID in internal format (1 - 31).          Bytes <b>4 - 7</b> = fabric configuration operation that failed.          Bytes <b>8 - 11</b> = fabric configuration step that failed.          Bytes <b>12 - 15</b> = managed switch domain ID in internal format (1 - 31).          Bytes <b>16 - 19</b> = response command code received from managed switch.          Bytes <b>20 - 23</b> = response code received from the managed switch.          Bytes <b>24 - 27</b> = reason code received from the managed switch.          Bytes <b>28 - 31</b> = error code received from the managed switch.</p>						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓				

## Power Supply Events (200 through 299)

Event Code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	Alternating current (AC) input to the indicated power supply is disconnected or AC circuitry in the power supply failed. The second power supply assumes the full operating load for the director.						
Action:	Ensure the power supply is connected to facility AC power, and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code <b>203</b> ), replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	Direct current (DC) circuitry in the power supply failed. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 202**

Message:	Power supply thermal failure.						
Severity:	Major.						
Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 203**

Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 204**

Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 206**

Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the director was powered on and operational. The second power supply assumes the full operating load for the director.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 207**

Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the director powered on and operational. Both power supplies adjust to share operating load for the director.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 208**

Message:	Power supply false shutdown.						
Severity:	Major.						
Explanation:	Director operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.						
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

## Fan Module Events (300 through 399)

Event Code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan module associated with the failed fan.						
Action:	Replace the indicated fan module.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte 0) specifies the failed fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 302**

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte <b>0</b> ) specifies the failed fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 303**

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Four cooling fans failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte <b>0</b> ) specifies the failed fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 304**

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Five cooling fans failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte <b>0</b> ) specifies the failed fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 305**

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Six cooling fans failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the fan modules associated with the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte <b>0</b> ) specifies the failed fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	



Event Code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan recovered or the associated fan module was replaced. One fan is operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 311							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans recovered or the associated fan modules were replaced. Two fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 312**

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans recovered or the associated fan modules were replaced. Three fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 313**

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Four cooling fans recovered or the associated fan modules were replaced. Four fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 314**

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans recovered or the associated fan modules were replaced. Five fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 315**

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Six cooling fans recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte 0) specifies the recovered fan numbers.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 320**

Message:	Fan module removed.						
Severity:	Major.						
Explanation:	A fan module was removed with the director powered on and operational.						
Action:	Replace the indicated fan module.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓				

**Event Code: 321**

Message:	Fan module installed.						
Severity:	Informational.						
Explanation:	A fan module was installed with the director powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 370							
Message:	Fan status polling temporarily disabled.						
Severity:	Minor.						
Explanation:	One or more fans are changing between failed or recovered status values beyond a threshold. One or more fans may have failed. These conditions will re-enable fan status polling: an IPL/IML/POR, enabled hourly, fan insertion.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

## CTP Card Events (400 through 499)

Event Code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a faulty field-replaceable unit (FRU) as indicated by the event data.						
Action:	Replace the failed FRU with a functional FRU. Perform the data collection procedure and return the CD and faulty FRU to McDATA support personnel.						
Event Data:	Byte <b>0</b> = FRU code as follows: <b>01</b> = backplane, <b>02</b> = CTP card, <b>03</b> = SBAR, <b>05</b> = fan module, <b>06</b> = power supply, and <b>08</b> through <b>0F</b> = UPMs. Byte <b>1</b> = FRU slot number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 410							
Message:	CTP card reset.						
Severity:	Informational.						
Explanation:	The indicated CTP card reset after a director power-on, CTP card installation, hardware IML (CTP card faceplate), or software IPL. An IPL can be user-initiated at the management server application, or occur automatically after a firmware fault (event code <b>411</b> ). The event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte <b>0</b> = reset type as follows: <b>00</b> = power-on or CTP hot-insert, <b>02</b> = IML, <b>04</b> = IPL, <b>40</b> = partition switch.						

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 411**

Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Firmware executing on the indicated CTP card encountered an unexpected operating condition and dumped the operating state to FLASH memory for retrieval and analysis. The dump file is automatically transferred from the director to the management server, where it is stored for retrieval through the data collection procedure. A non-disruptive failover to the backup CTP card occurs. When the dump and subsequent IPL complete, the faulty CTP card re-initializes to become a the backup.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Bytes <b>0 - 3</b> = fault identifier, least significant byte first.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓	✓	✓	✓	

**Event Code: 412**

Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform the data collection procedure and return the CD to McDATA support personnel.						
Event Data:	Byte <b>0</b> = reset type as follows: <b>00</b> = task switch did not occur within approximately one second, <b>01</b> = interrupt servicing blocked for more than approximately one second.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 413**

Message:	Backup CTP card POST failure.						
Severity:	Major.						
Explanation:	A backup CTP card was installed in the director and failed POSTs.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	



Event Code: 414							
Message:	Backup CTP card failure.						
Severity:	Major.						
Explanation:	The backup CTP card failed.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 415							
Message:	Backup CTP card removed.						
Severity:	Informational.						
Explanation:	The backup CTP card was removed while the director was powered on and operational.						
Action:	Install an operational backup CTP card.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 416**

Message:	Backup CTP card installed.						
Severity:	Informational.						
Explanation:	A backup CTP card was installed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 417**

Message:	CTP card firmware synchronization initiated.						
Severity:	Informational.						
Explanation:	The active CTP card initiated a firmware synchronization with the backup CTP card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 418							
Message:	User-initiated CTP card switchover.						
Severity:	Informational.						
Explanation:	The backup CTP card became the active CTP card after a user-initiated switchover. The previously active CTP card is now the backup CTP card.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 420							
Message:	Backup CTP card NVRAM failure.						
Severity:	Major.						
Explanation:	The backup CTP card detected a NVRAM memory failure. The failure has no impact on the active CTP card.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = NVRAM area identifier.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 421**

Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A director firmware version was downloaded from the management server or Web server. The event data indicates the firmware version in hexadecimal format <b>xx.yy.zz bbbb</b> , where <b>xx</b> is the release level, <b>yy</b> is the maintenance level, <b>zz</b> is the interim release level, and <b>bbbb</b> is the build ID.						
Action:	No action required.						
Event Data:	Bytes <b>0</b> and <b>1</b> = release level ( <b>xx</b> ). Byte <b>2</b> = always a period. Bytes <b>3</b> and <b>4</b> = maintenance level ( <b>yy</b> ). Byte <b>5</b> = always a period. Bytes <b>6</b> and <b>7</b> = interim release level ( <b>zz</b> ). Byte <b>8</b> = always a space. Bytes <b>9 - 12</b> = build ID ( <b>bbbb</b> ).						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 422**

Message:	CTP firmware synchronization complete.						
Severity:	Informational.						
Explanation:	Active CTP card synchronization with the backup CTP card complete.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The management server or Web server initiated download of a new firmware version to the director.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 426							
Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a <b>426</b> event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte <b>0</b> of the event data (equal to <b>5</b> , <b>10</b> , <b>15</b> , or <b>20</b> ) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to <b>10</b> indicates 1,024 ECC error interrupts.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 427**

Message:	Utility bus error detected by backup CTP.						
Severity:	Major.						
Explanation:	Backup CTP is unable to communicate with one or more port modules due to errors in its utility bus. Director may not be fully operational if backup CTP becomes master CTP.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Each byte of data represents the ID of the port module with which the backup CTP was unable to communicate.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
			✓				

**Event Code: 433**

Message:	Non-recoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable error was detected on the CTP card Ethernet adapter and the LAN connection to the management server or Internet terminated. All Fibre Channel switching functions remain unaffected. This event only occurs on a director with a single CTP card. Because Ethernet communication is lost, no failure indication is externally reported.						
Action:	Replace the CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Bytes <b>0 - 3</b> = LAN error type, where <b>01</b> = hard failure and <b>04</b> = registered fault. Bytes <b>4 - 7</b> = LAN error subtype (internally defined). Bytes <b>8 - 11</b> = LAN fault identifier (internally defined).						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓				✓	

Event Code: 440							
Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal CTP card error.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = CTP slot position. Byte 1 = engineering reason code Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP card detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte 0 = port number. Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = high-availability error callout #1. Bytes 10 and 11 = high-availability error callout #2. Byte 12 = detecting port. Byte 13 = connected port. Byte 14 = participating SBAR. Bytes 16 and 17 = high-availability error callout #3. Bytes 18 and 19 = high-availability error callout #4.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 450							
Message:	Serial number mismatch detected.						
Severity:	Informational.						
Explanation:	This event occurs when the sequence number or OEM serial number in the system VPD (read from the backplane) does not match the sequence number and serial number that was saved in NVRAM the last time the director was IPLed. This event will occur normally when a CTP is moved from one switch to the master position of another switch. This event may occur abnormally when a hardware problem causes a problem reading the system VPD from the backplane.						
Action:	None. Any configured feature keys will be cleared. Configuration information will be synched with the backplane VPD, and the CTP will automatically be IPLed.						
Event Data:	Bytes <b>0 - 12</b> = sequence number from the system VPD. Bytes <b>13 - 31</b> = OEM serial number from the system VPD.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				



Event Code: 453							
Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the management server or Web server. The director performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	<p>Byte 0 = feature description as follows: <b>00</b> through <b>04</b> = Flexport, <b>06</b> = open-system management server, <b>07</b> = FICON management server.</p> <p>Byte 1 = feature description as follows: <b>01</b> = full volatility, <b>02</b> = FICON CUP zoning, <b>03</b> = SANtegrity authentication, <b>04</b> = CNT support, <b>05</b> = hardware trunking, <b>06</b> = SANtegrity binding, <b>07</b> = open trunking</p> <p>Byte 2 = feature description as follows: <b>02</b> = remote fabric license, <b>06</b> = Element Manager license, <b>07</b> = preferred path</p>						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

## Port Card (UPM and XPM) Events (500 through 599)

Event Code: 500							
Message:	Port card hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of a UPM was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the UPM, but the card is not seated. When the card is seated in the director chassis and identified by firmware, an event code <b>501</b> is generated.						
Action:	If event code <b>501</b> follows this event and the amber LED on the UPM extinguishes, the replacement card is installed and no additional action is required. If event code <b>501</b> does not follow this event, re-seat the UPM. If event code <b>501</b> still does not appear, replace the UPM.						
Event Data:	Byte <b>0</b> = UPM slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 501							
Message:	Port card recognized.						
Severity:	Informational.						
Explanation:	A UPM is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte <b>0</b> = UPM slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 502							
Message:	Port module anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP card detected a deviation in the normal operating mode or status of the indicated four-port UPM.						
Action:	No action required. An event code <b>504</b> is generated if the UPM fails.						
Event Data:	Byte <b>0</b> = UPM slot position. Byte <b>1</b> = engineering reason code. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8</b> and <b>9</b> = high-availability error callout #1. Bytes <b>10</b> and <b>11</b> = high-availability error callout #2. Byte <b>14</b> = participating SBAR. Bytes <b>16</b> and <b>17</b> = high-availability error callout #3. Bytes <b>18</b> and <b>19</b> = high-availability error callout #4.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 503							
Message:	Port card hot-removal completed.						
Severity:	Informational.						
Explanation:	A UPM was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte <b>0</b> = UPM slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 504**

Message:	Port module failure.						
Severity:	Major.						
Explanation:	The indicated UPM failed.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = UPM slot position. Byte 1 = engineering reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = reason code specific data.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 505**

Message:	Port module revision not supported.						
Severity:	Minor.						
Explanation:	The indicated UPM is not recognized and the four ports appear uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the UPM with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = UPM slot position. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 506							
Message:	Fibre Channel port failure.						
Severity:	Major.						
Explanation:	A Fibre channel port on a UPM failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte <b>0</b> = port number. Byte <b>1</b> = engineering reason code. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8 - 11</b> = reason code specific. Byte <b>16</b> = connector type. Bytes <b>17 and 18</b> = transmitter technology. Byte <b>19</b> = distance capabilities. Byte <b>20</b> = supported transmission media. Bytes <b>21 and 22</b> = speed capability and configuration.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 507**

Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code <b>506</b> is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte <b>0</b> = port number. Byte <b>1</b> = engineering reason code. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8 - 11</b> = reason code specific. Byte <b>12</b> = test type.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 508**

Message:	Fibre Channel port anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP card detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.						
Action:	No action required. An event code <b>506</b> is generated if this anomaly results in a hard port failure.						
Event Data:	Byte <b>0</b> = port number. Byte <b>1</b> = anomaly reason code. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8</b> and <b>9</b> = high-availability error callout #1. Bytes <b>10</b> and <b>11</b> = high-availability error callout #2. Byte <b>12</b> = detecting port. Byte <b>13</b> = connected port. Byte <b>14</b> = participating SBAR. Bytes <b>16</b> and <b>17</b> = high-availability error callout #3. Bytes <b>18</b> and <b>19</b> = high-availability error callout #4.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 509							
Message:	Fibre Channel path failure.						
Severity:	Major.						
Explanation:	<p>One or more of the backplane data paths has been removed from service, thus reducing the bandwidth capabilities of the associated port. This does not prevent the port from frame reception or transmission, but it does limit the potential throughput of the port.</p> <p>Normally the amber Service Required LED on the port associated with the failing path is illuminated to indicate the degraded status. The green port LED may or may not be illuminated based on the status of the link.</p>						
Action:	<p>Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.</p> <p>A failed path may also be recovered by performing a port reset with the SAN management application, however any newly detected errors may cause the path to re-fail.</p>						
Event Data:	<p>Byte 0 = port number.</p> <p>Byte 1 = engineering reason code.</p> <p>Bytes 4 - 7 = elapsed millisecond tick count.</p>						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 510**

Message:	SFP/XFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an SFP or XFP optical transceiver was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte 0 = port number. Byte 2 = type of optics: Bit 1 = SFP; Bit 2 = XFP. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 512**

Message:	SFP/XFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Director firmware detected an SFP or XFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number. Byte 2 = type of optics: Bit 1 = SFP; Bit 2 = XFP. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				



**Event Code: 513**

Message:	SFP/XFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP or XFP optical transceiver was removed while the director was powered on and operational.						
Action:	No action required.						
Event Data:	Byte 0 = port number. Byte 2 = type of optics: Bit 1 = SFP; Bit 2 = XFP. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 514**

Message:	SFP/XFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP or XFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte 0 = port number. Byte 2 = type of optics: Bit 1 = SFP; Bit 2 = XFP. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 515**

Message:	SFP/XFP optics digital diagnostics warning threshold exceeded.						
Severity:	Minor.						
Explanation:	A digital diagnostics warning threshold is exceeded. If warning condition persists, additional <b>515</b> events are generated.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte <b>0</b> = port number. Byte <b>2</b> = type of optics: Bit <b>1</b> = SFP; Bit <b>2</b> = XFP. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 516**

Message:	SFP/XFP optics digital diagnostics alarm threshold exceeded.						
Severity:	Minor.						
Explanation:	A digital diagnostics warning threshold is exceeded. If warning condition persists, additional <b>516</b> events are generated.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte <b>0</b> = port number. Byte <b>2</b> = type of optics: Bit <b>1</b> = SFP; Bit <b>2</b> = XFP. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 519							
Message:	Port module ASIC reset.						
Severity:	Information.						
Explanation:	System software detected an abnormal event associated with the port module. Recovery of the port module required system software to perform a reset of the port module hardware.						
Action:	Monitor the performance of the port module (and associated port modules). If persistent resets occur, or if other system errors are recorded against the module, replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = slot number. Byte 1 = engineering reset reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 570							
Message:	Link recovery action.						
Severity:	Informational.						
Explanation:	Link recovery was performed by E/OS firmware to recover an unsuitable link.						
Action:	Check port statistics invalid transmission words and CRC errors. Verify that the attached device is honoring the buffer-to-buffer flow control protocol as described in the FC-FS standard.						
Event Data:	Byte 0 = port number. Byte 1 = link recovery reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 581**

Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached open systems interconnection (OSI) or Fibre Connection (FICON) server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

**Event Code: 582**

Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

Event Code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

**Event Code: 585**

Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

**Event Code: 586**

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI or FICON server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI) or the FICON architecture document (FICON). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. See <a href="#">MAP 0000: Start MAP</a> on page 3-9 for instructions.						
Event Data:	Refer to the T11/99-017v0 or FICON architecture document for the specific link incident record format.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
							✓

## SBAR Events (600 through 699)

Event Code: 600							
Message:	SBAR hot-insertion initiated.						
Severity:	Informational						
Explanation:	Installation of a backup SBAR was initiated with the director powered on and operational. The event indicates that operational firmware detected the presence of the SBAR, but the SBAR is not seated. When the SBAR is seated in the director chassis and identified by firmware, an event code <b>601</b> is generated.						
Action:	If event code <b>601</b> follows this event and the amber LED on the SBAR extinguishes, the replacement SBAR is installed and no additional action is required. If event code <b>601</b> does not follow this event, re-seat the SBAR. If event code <b>601</b> still does not appear, replace the SBAR.						
Event Data:	Byte <b>0</b> = SBAR slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 601							
Message:	SBAR hot-insertion completed.						
Severity:	Informational.						
Explanation:	An SBAR is installed and recognized by director operational firmware.						
Action:	No action required.						
Event Data:	Byte <b>0</b> = SBAR slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 602**

Message:	SBAR anomaly detected.						
Severity:	Informational.						
Explanation:	Director operational firmware detected a deviation in the normal operating mode or operating status of the indicated SBAR.						
Action:	No action required. An event code <b>604</b> is generated if the SBAR fails.						
Event Data:	Byte <b>0</b> = SBAR slot position. Byte <b>1</b> = anomaly reason code. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8 and 9</b> = high-availability error callout #1. Bytes <b>10 and 11</b> = high-availability error callout #2.						
	Byte <b>12</b> = detecting port. Byte <b>13</b> = connected port. Byte <b>14</b> = participating SBAR. Bytes <b>16 and 17</b> = high-availability error callout #3. Bytes <b>18 and 19</b> = high-availability error callout #4.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 603**

Message:	SBAR hot-removal completed.						
Severity:	Informational.						
Explanation:	An SBAR was removed with the director powered on and operational.						
Action:	No action required.						
Event Data:	Byte <b>0</b> = SBAR slot position. Bytes <b>4 - 7</b> = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				



Event Code: 604							
Message:	SBAR failure.						
Severity:	Major.						
Explanation:	The indicated SBAR failed. If the active SBAR fails, the backup SBAR takes over operation. If the backup SBAR fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to McDATA support personnel.						
Event Data:	Byte 0 = SBAR slot position. Byte 1 = engineering failure reason code. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 - 11 = event code specific data.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 605							
Message:	SBAR revision not supported.						
Severity:	Minor.						
Explanation:	The indicated SBAR is not recognized and appears uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to McDATA support personnel.						
Event Data:	Byte 0 = SBAR slot position. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = detected module identifier.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

**Event Code: 607**

Message:	Director contains no operational SBARs.						
Severity:	Severe.						
Explanation:	The director firmware does not recognize an installed SBAR.						
Action:	Install at least one functional SBAR and power-on reset (POR) the director.						
Event Data:	Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓		

**Event Code: 608**

Message:	User initiated SBAR switch-over.						
Severity:	Informational.						
Explanation:	The backup SBAR has become the active SBAR at a user's request. The previously active SBAR is now the backup SBAR.						
Action:	No action required.						
Event Data:	There is no supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 619							
Message:	SBAR module ASIC reset.						
Severity:	Informational.						
Explanation:	System software detected an abnormal event associated with the SBAR. Recovery of the SBAR required system software to perform a reset of the port module hardware.						
Action:	Monitor the performance of the SBAR. If persistent resets occur, or if other system errors are recorded against the module, replace the indicated SBAR with a functional SBAR. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	Byte 0 = SBAR slot position. Byte 1 = engineering reset reason code. Bytes 4 - 7 = elapsed millisecond tick count.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 620							
Message:	SBAR fan failure.						
Severity:	Informational.						
Explanation:	System software has detected the failure of one or more SBAR fan modules.						
Action:	No direct action required. System software continues monitoring the SBAR thermal status. In the event of a detected thermal violation, subsequent <b>805</b> , <b>806</b> , or <b>807</b> events will be posted.						
Event Data:	Bytes 0 - 3 = reserved. Bytes 4 - 7 = elapsed millisecond tick count. Bytes 8 and 9 = failed SBAR fan count. Bytes 10 and 11 = operational SBAR fan count. Byte 12 - 15 = reserved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

Event Code: 621							
Message:	Failed SBAR fan recovered.						
Severity:	Informational.						
Explanation:	System software has detected that one or more failed SBAR fan modules has recovered.						
Action:	None.						
Event Data:	Bytes <b>0 - 3</b> = reserved. Bytes <b>4 - 7</b> = elapsed millisecond tick count. Bytes <b>8</b> and <b>9</b> = failed SBAR fan count. Bytes <b>10</b> and <b>11</b> = operational SBAR fan count. Byte <b>12 - 15</b> = reserved.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓		✓				

## Thermal Events (800 through 899)

Event Code: 800							
Message:	High temperature warning (port module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 801							
Message:	Critically hot temperature warning (port module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 802**

Message:	Port module shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A UPM failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code <b>801</b> ).						
Action:	Replace the failed UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 805**

Message:	High temperature warning (SBAR thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 806							
Message:	Critically hot temperature warning (SBAR thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 807							
Message:	SBAR shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An SBAR failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code <b>806</b> ). If the active SBAR fails, the backup SBAR takes over operation. If the backup SBAR fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 810**

Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

**Event Code: 811**

Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	



Event Code: 812							
Message:	CTP card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A CTP card failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code <b>811</b> ). If the active CTP card fails, the backup card takes over operation. If the backup CTP card fails, the active card is not impacted.						
Action:	Replace the failed CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	

Event Code: 850							
Message:	System shutdown due to CTP card thermal violations.						
Severity:	Severe.						
Explanation:	The director powered off because of excessive thermal violations on the last operational CTP card.						
Action:	Replace the failed CTP card with a functional card. Perform the data collection procedure and return the CD and faulty card to McDATA support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✓	✓	✓	✓	✓	✓	



## Director Specifications

This appendix lists physical characteristics, storage and shipping environment, and operating environment for the Intrepid 6140 Director.

### Physical Characteristics

#### Dimensions:

**Height:** 52.9 centimeters (20.8 inches) or 12 rack units

**Width:** 44.5 centimeters (17.5 inches)

**Depth:** 61.3 centimeters. (24.1 inches)

**Weight:** 75.9 kilograms (167.0 pounds)

#### Power requirements:

**Input voltage:** 200 to 240 VAC

**Input current:** 4.2 amps at 208 VAC

**Input frequency:** 47 to 63 Hz

Plan for single phase or phase-to-phase connections and 15-ampere dedicated service

#### Heat dissipation:

Nominal: 841 watts (2,873 BTUs/hr)

#### Cooling airflow clearances (director chassis):

**Right and left side:** 2.5 centimeters (1.0 inches)

**Front and rear:** 7.6 centimeters (3.0 inches)

---

**Shipping and  
Storage  
Environment**

**Top and bottom:** No clearance required

**Acoustical noise:**

70.0 dB "A" scale

Protective packaging must be provided to protect the director under all shipping methods (domestic and international).

**Shipping temperature:**

-40° C to 60° C (-40° F to 140° F)

**Storage temperature:**

1° C to 60° C (34° F to 140° F)

**Shipping relative humidity:**

5% to 100%

**Storage relative humidity:**

5% to 80%

**Maximum wet-bulb temperature:**

29° C (84° F)

**Altitude:**

12,192 meters (40,000 feet)

---

**Operating  
Environment**

**Temperature:**

4° C to 40° C (40° F to 104° F)

**Relative humidity:**

8% to 80%

**Maximum wet-bulb temperature:**

27° C (81° F)

**Altitude:**

3,048 meters (10,000 feet)

**Inclination:**

10° maximum

**Fabricenter  
Equipment Cabinet  
Service Clearances**

- Front:** 91.4 centimeters (36.0 inches)
- Rear:** 91.4 centimeters (36.0 inches)
- Right side:** No clearance required
- Left side:** No clearance required



## Management Server and Ethernet Hub

This appendix describes the management server and the optional, Ethernet hub.

### Management Server Description

The management server with a liquid crystal display (LCD) panel ([Figure D-1](#)) is a one rack unit (1U) high, LAN-accessed, rack-mount unit that provides a central point of control for up to 48 connected directors, switches, or other McDATA managed products. Server applications are accessed through a LAN-attached PC or workstation with client software installed.



**Figure D-1 Management Server**

The server is rack mounted in the McDATA FC-512 Fabriccenter equipment cabinet. The management server or CLI is required to install, configure, and manage the director.

The management server provides two auto-detecting 10/100 Mbps Ethernet LAN connectors (RJ-45 adapters). The first adapter (LAN 1) can be attached to a public customer intranet to allow access from

remote user workstations. The second adapter (LAN 2) attaches to a private LAN segment containing directors, switches, or other managed McDATA products.

---

## Management Server Specifications

The following list summarizes the hardware specifications for the management server platform. Some platforms may ship with more enhanced hardware, such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive.

- 1U rack-mount server running the Intel® Pentium® 4 processor with an 1,800 megahertz (MHz) or greater clock speed, Microsoft Windows® 2000 Professional operating system, and power cord.
- TightVNC Viewer Version 1.2.7 client-server software control package that provides remote network access (through a standard web browser) to the management server desktop.
- 1,024 megabyte (MB) or greater RAM.
- 40 gigabyte (GB) or greater internal hard drive.
- 1.44 MB 3.5-inch slim-type disk drive and slim-type compact disk-rewritable (CD-RW) drive.
- 56K internal modem.
- Two 10/100 Mbps Ethernet adapters with RJ-45 connectors.

---

## Ethernet Hub Description

The management server and managed directors or switches connect through a 10/100 Base-T McDATA-qualified Ethernet hub ([Figure D-2](#)).





**Figure D-2 24-Port Ethernet Hub**

Hubs can be daisy-chained to provide additional connections as more directors or switches (or other McDATA managed products) are installed on a network. Multiple hubs are daisy-chained by attaching RJ-45 Ethernet patch cables and configuring each hub through a medium-dependent interface (MDI) switch.



## Restore Management Server

The procedure in this appendix provides information to restore the rack-mount management server after a failure of the server hard drive. The procedure includes restoration of the:

- Windows 2000 Professional operating system.
- Windows 2000 configuration information.
- Storage area network (SAN) management application (EFCM or SANavigator) and Intrepid 6140 Element Manager application.
- SAN management application data directory.

### Requirements

The following are required to perform this procedure:

- **Management Server Restore CD-ROM** - This CD-ROM is shipped with the management server and contains the:
  - Disk operating system (DOS) files required to boot the PC after a hard drive failure.
  - Windows 2000 Professional operating system.
- **EFC Management Applications CD-ROM** - This CD-ROM contains the SAN management application (EFCM or SANavigator) and Intrepid 6140 Element Manager application.

- **SAN management data directory backup on CD-ROM** - The SAN management data directory is automatically backed up to a CD when the management server is rebooted or when the data directory contents change. The data directory includes:
  - All configuration data (product definitions, user names, passwords, user rights, nicknames, session options, SNMP trap recipients, E-mail recipients, and Ethernet event notifications).
  - All log files (SAN management application and Element Manager logs).
  - Zoning library (all zone set and zone definitions).
  - Firmware library.
  - Call-home settings.
  - Configuration data for each managed Intrepid 6140 Director (stored on the server and in NV-RAM on each director or switch).
- **Windows 2000 configuration information** - Windows 2000 network addresses, date and time information, user information, and the product identification are recorded during installation of the management server ([Subtask F: Record or Verify Management Server Restore Information](#) on page 2-39).

---

## Restore Management Server Procedure


To restore the rack-mount management server:

1. At the server, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
2. Insert the *Management Server Restore* CD-ROM in the CD-RW drive and close the LCD panel.

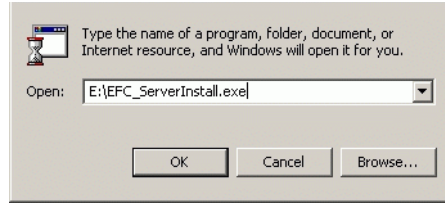
---

**ATTENTION!** This procedure deletes all data from the C: hard drive partition.

---

3. Press the power () button. The server powers on and performs a restore from the CD-ROM.

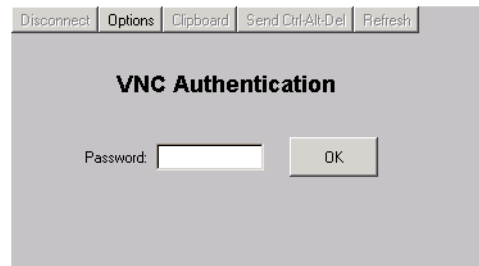
4. After the restore completes, the server makes a series of beeps. Remove the *Management Server Restore* CD-ROM from the CD-RW drive.
5. Power cycle the server. The server performs power-on self-tests (POSTs). After successful POST completion, the LCD panel displays a **Welcome!!** message, then cycles through and displays server operational information.
6. Configure the following parameters at the server LCD panel (*Subtask A: Configure Password and Network Addresses* on page 2-22).
  - LCD panel password.
  - IP address for private and public LAN connections.
  - Subnet mask or private and public LAN connections.
7. Log on to the server Windows 2000 desktop through a LAN connection to a browser-capable PC (*Access the Management Server Desktop* on page 2-26).
8. Configure Windows 2000 configuration information as required by the customer:
  - a. Configure the computer and workgroup names for the server. If required, change the server gateway address and DNS server IP address to conform to the customer LAN addressing plan (*Subtask B: Configure Management Server Information* on page 2-25).
  - b. Change the default Windows 2000 administrator password and configure password access for authorized users (*Subtask C: Configure Windows 2000 Users* on page 2-30).
  - c. Set the server date and time (*Subtask D: Set Management Server Date and Time* on page 2-36).
  - d. Configure the call-home feature (*Subtask E: Configure the Call-Home Feature* on page 2-38).
9. Insert the *EFC Management Applications* CD-ROM in the CD-RW drive and close the LCD panel.
10. At the server Windows 2000 desktop, click *Start* at the left side of the task bar, then select the *Run* option. The *Run* dialog box displays (*Figure E-1*).



**Figure E-1 Run Dialog Box**

11. At the *Run* dialog box, type **D:\mcdDataServerInstall** in the *Open* field.
12. Click *OK*. A series of message boxes appear as the *InstallAnywhere* third-party application prepares to install the SAN management software, followed by the *McDATA EFC Management Applications* dialog box.
13. Follow the online instructions for the *InstallAnywhere* program. Click *Next*, *Install*, or *Done* as appropriate.
14. Remove the *EFC Management Applications* CD-ROM from the CD-RW drive.
15. Insert SAN management data directory backup CD-ROM (created while performing [Task 9: Configure SANtegrity Authentication \(Optional\)](#) on page 2-77) in the CD-RW drive and close the LCD panel.
16. Copy the contents of the CD-ROM to the server hard drive:
  - For the EFCM 8.5 application, copy the CD-ROM contents to the following directories:
    - **C:\Program Files\EFCM 8.5\CallHome**
    - **C:\Program Files\EFCM 8.5\Client**
    - **C:\Program Files\EFCM 8.5\Server.**
  - For the Sanavigator 4.1 application, copy the CD-ROM contents to the following directories:
    - **C:\Program Files\SANavigator4.1\CallHome**
    - **C:\Program Files\SANavigator4.1\Client**
    - **C:\Program Files\SANavigator4.1\Server.**

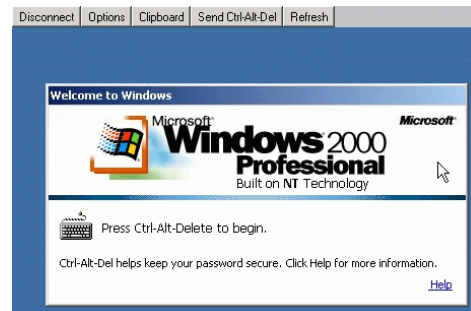
17. Power off and reboot the server.
  - a. At the Windows 2000 desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box displays.
  - b. Select the *Restart* option from the list box and click *OK*. The server powers down and restarts. During the reboot, the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.
  - c. After the server reboots, click *Login again*. The *VNC Authentication* screen displays (Figure E-2).



**Figure E-2 VNC Authentication Screen**

- d. Type the default password and click *OK*. The *Welcome to Windows* dialog box displays (Figure E-3).

**NOTE:** The default TightVNC viewer password is **password**.



**Figure E-3 Welcome to Windows Dialog Box**

- e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box displays (Figure E-4).

---

**NOTE:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**. This action logs the user on to the browser-capable PC, not the management server.

---



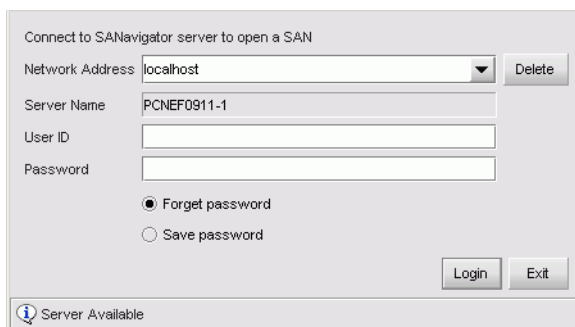
**Figure E-4 Log On to Windows Dialog Box**

- f. Type the default Windows 2000 user name and password and click **OK**. The server Windows 2000 desktop opens and the *EFCM Log In* or *SANavigator Log In* dialog box displays (Figure E-5).

---

**NOTE:** The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---



**Figure E-5 EFCM Log In or SANavigator Log In Log In Dialog Box**



- g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

---

**NOTE:** The default SAN management application user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

---

- h. Click *Login*. The application opens and the EFCM or SANavigator main window appears.



## Safety Notices (Multi-Lingual Translations)

The **DANGER** and **CAUTION** safety notices in this publication are provided in the following languages:

- English
- Chinese, Simplified (PRC China)
- Chinese, Traditional (ROC Taiwan)
- French
- German
- Hebrew
- Italian
- Portuguese (Brazil)
- Spanish
- Spanish (Latin America)

**DANGER**

*Use the supplied power cords. Ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.*

**DANGER**

*Disconnect the power cords.*

**CAUTION**

*Use safe lifting practices when moving the product.*

**危險**

*使用所提供的电源线。確保使用正確型號的設備電源插座，提供必需的電壓並且正確接地。*

**危險**

*拔除電源線。*



小心

搬运产品时务求安全。



危險

使用隨附的電源線，確定使用正確類型的設備電源插座，  
提供必需的電壓，並且正確接地。



危險

拔除電源線。



注意

搬運產品時務求安全。

**DANGER**

*Utiliser les câbles d'alimentation fournis. S'assurer que la prise de courant du local est du type correct, délivre la tension requise et est correctement raccordée à la terre.*

**DANGER**

*Débrancher les câbles d'alimentation.*

**ATTENTION**

*Utiliser des techniques de levage sûres pour déplacer le produit.*

**GEFAHR**

*Die mitgelieferten Netzkabel verwenden. Sicherstellen, dass die verwendete Netzsteckdose dem vorgeschriebenen Typ entspricht, die erforderliche Spannung liefert und einwandfrei geerdet ist.*

**GEFAHR**

*Netzkabel abziehen.*

**VORSICHT**

*Beim Bewegen des Produktes auf eine sichere Hubtechnik achten.*



### סכנה

השתמש בכבלי החשמל הנלווים. וודא כי כלי הקיבול לחשמל של המתקן הוא מהסוג הנכון, מספק את המתח הדרוש, ומוארק כהלכה.



### סכנה

נתק את כבלי החשמל.



### זהירות

נהג ע"פ נהלי הרמה בטיחותיים בעת הזת המוצר.



### PERICOLO

*Usare il cavo di alimentazione in dotazione. Assicurarsi che la presa di corrente a disposizione sia del tipo corretto, eroghi la tensione richiesta e sia dotata di messa a terra idonea.*



### PERICOLO

*Scollegare tutti i cavi di alimentazione.*



### ATTENZIONE

*Sollevare il prodotto con prudenza per evitare di infortunarsi.*

**PERIGO**

*Use os cordões elétricos fornecidos. Certifique-se de que o tipo de receptor de energia da facilidade é apropriado, fornece a voltagem necessária, e está corretamente aterrado.*

**PERIGO**

*Desconecte os cordões elétricos.*

**CUIDADO**

*Use práticas de levantamento seguras ao mover o produto.*

**PELIGRO**

*Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea del tipo correcto, suministre el voltaje necesario, y que esté apropiadamente conectado a tierra.*

**PELIGRO**

*Desconecte los cables de alimentación.*

**PRECAUCIÓN**

*Tenga mucho cuidado al levantar el producto para moverlo.*



**PELIGRO**

*Utilice los cables de alimentación proporcionados. Asegúrese que el receptáculo tomacorriente para la instalación sea el tipo correcto, suministre el voltaje necesario, y que esté apropiadamente puesto a tierra.*

**PELIGRO**

*Desconecte los cables de alimentación.*

**PRECAUCIÓN**

*Tenga mucho cuidado al levantar el producto para moverlo.*



This glossary defines terms used in this manual or terms related to the product. It is not a comprehensive glossary of computer terms.

The following cross-references are used in this glossary:

*Contrast with.* This refers to a term that has an opposite or substantively different meaning.

*See.* This refers the reader to another keyword or phrase for the same term.

*See also.* This refers the reader to definite additional information contained in another entry.

## NUMERICS

**10BaseT** An implementation of the IEEE Ethernet standard for 24-gauge unshielded twisted-pair wiring, using a baseband transmission rate of ten Mbps.

**100BaseT** An implementation of the IEEE Ethernet standard for 24-gauge unshielded twisted-pair wiring, using a baseband transmission rate of 100 Mbps.

**10 Gbps form factor pluggable transceiver** A laser-driven 10 Gbps form factor optical transceiver used for a wide range of networking applications requiring high data rates (usually 10 Gbps). XFP transceivers provide port connectivity for Intrepid-series directors.

**10 Gbps port module card** A printed circuit board (Intrepid-series directors only) that provides port connections that support 10.625 Gbps Fibre Channel communication. Port connectivity is provided through XFP optical transceivers. *Contrast with [fibre port module card](#) and [universal port module card](#).*

## A

**active zone set** The zone set active for a multiswitch fabric, and created when a user-specified zone set is enabled. *See also [zone](#) and [zone set](#).*

**AL\_PA** *See [arbitrated loop physical address](#).*

**application** (1) An information processing system, for example, a payroll application, an airline reservation application, or a network application. (2) Software used to perform specific types of user-oriented work on a computer.

**arbitrated loop** One of three topologies offered by the Fibre Channel protocol. The topology is structured as a loop and requires an attached port to successfully arbitrate for access prior to establishing a circuit to transmit or receive frames. *See also [switched fabric](#) and [point-to-point](#).*

**arbitrated loop physical address** A single-byte value used to identify physical port addresses on an arbitrated loop. An arbitrated loop has one FL\_Port address and 126 NL\_Port addresses (127 valid AL\_PAs).

**arbitration** The process of selecting one respondent from a collection of several candidates that request service concurrently.

**Audit Log** A log that summarizing actions (audit trail) performed on a managed product through the director or switch-specific Element Manager application or an SNMP workstation. *Contrast with [EFC Audit Log](#).*

## B

**bandwidth** (1) The difference (expressed in Hertz) between the highest and lowest frequencies in a range of frequencies. (2) The data transfer rate of a network or electronic communication system.

<b>BB_Credit</b>	See <i>buffer-to-buffer credit</i> .
<b>beaconing</b>	The use of light-emitting diodes on ports, port cards, FRUs, directors, and switches to aid in the fault-isolation process. When enabled, beaconing causes amber LEDs to flash.
<b>BER</b>	See <i>bit error rate</i> .
<b>bidirectional</b>	The capability to simultaneously communicate in both directions over a single connection, with flow control. <i>Synonymous with full-duplex</i> .
<b>bit</b>	A digital 0 or 1, and abbreviated with a lower case <b>b</b> . Synonymous with binary digit. <i>Contrast with byte</i> .
<b>bit error rate</b>	The number of bits received incorrectly divided by the total number of bits transmitted.
<b>B_Port</b>	See <i>bridge port</i> .
<b>bps</b>	Acronym for bits per second. <i>Contrast with Bps</i> .
<b>Bps</b>	Acronym for bytes per second. <i>Contrast with bps</i> .
<b>bridge port</b>	In Fibre Channel protocol, a port that connects a bridge device with a director or switch expansion port (E_Port) to form an ISL. B_Ports provide a subset of E_Port functionality. The McDATA ES-1000 Switch connects to directors and fabric switches through a B_Port. <i>See also expansion port</i> .
<b>broadcast</b>	In Fibre Channel protocol, to send a transmission to all device node ports (N_Ports) attached to a fabric.
<b>buffer-to-buffer credit</b>	The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port), and representing the maximum number of frames transmitted by the N_Port or F_Port without causing a buffer overrun at the receiving port. The value is adjustable to provide different levels of buffering.
<b>byte</b>	A binary character consisting of eight bits, and abbreviated with an upper case <b>B</b> . Synonymous with octet. <i>Contrast with bit</i> .

## C

<b>call-home</b>	A configurable director or switch feature that enables the attached management server to automatically contact a support center and report system problems.
<b>central memory module card</b>	A printed circuit board (ED-5000 Director only) that provides the storage area for director ports to deposit and retrieve Fibre Channel frames. Each port is allocated a portion of this memory, divided into a fixed number of frame buffers.
<b>Class 2 Fibre Channel service</b>	Provides connectionless multiplexed Fibre Channel service between fabric-attached node ports (N_Ports) with acknowledgement of frame delivery or nondelivery. Class 2 service is best suited for mainstream computing applications.
<b>Class 3 Fibre Channel service</b>	Provides connectionless multiplexed Fibre Channel service between fabric-attached node ports (N_Ports) without acknowledgement of frame delivery or nondelivery. Class 3 service is best suited for storage or video applications.
<b>Class F Fibre Channel service</b>	Used by directors, switches, or other fabric elements to communicate across ISLs to configure, control, and coordinate a multiswitch fabric.
<b>cluster</b>	A group of Fibre Channel directors and switches configured as a single entity and managed through the Cluster Manager application.
<b>Cluster Log</b>	A log recorded at the Cluster Manager application that displays a history of cluster-related events, particularly events related to configuration inconsistencies.
<b>Cluster Manager application</b>	An application providing the management and graphical user interface for a user-specified cluster of directors and switches. Each instance of the Cluster Manager application is opened from the EFC Manager application. The application runs locally on the management server and can be downloaded to remote user workstations. <i>See also <a href="#">EFC Manager application</a> and <a href="#">Element Manager application</a>.</i>
<b>CMM card</b>	<i>See <a href="#">central memory module card</a>.</i>
<b>concurrent maintenance</b>	The ability to perform maintenance tasks, such as FRU removal and replacement or firmware downloads, while a director or switch is powered on and operational.

<b>configuration data</b>	A collection of data that results from configuring director, switch, and system operating parameters. Configuration data includes product identification, port configurations, operating parameters, SNMP configuration, and zoning configuration. A backup file is required to restore configuration data if the CTP card in a nonredundant director is removed and replaced.
<b>connectionless</b>	A nondedicated link between fabric-attached nodes that allows a director or switch to forward Class 2 or Class 3 Fibre Channel frames as resources (ports) allow.
<b>control processor card</b>	A printed circuit board that provides the microprocessor and control logic for all directors and switches. The CTP card also initializes hardware components after system power-on. The board may also provide an RJ-45 Ethernet connector.
<b>control unit port</b>	An internal director or switch port, embedded on the CTP card, that communicates with channels to report errors and link initialization.
<b>CTP card</b>	See <i>control processor card</i> .
<b>CUP</b>	See <i>control unit port</i> .
<b>D</b>	
<b>DB-9 connector</b>	A 9-pin serial connector type that provides connectivity to an ES-1000 Switch GBIC. Contrast with <i>high speed serial data connector</i> .
<b>default zone</b>	A zone that contains all fabric-attached devices not configured as members of a user-specified zone in the active zone set.
<b>D_ID</b>	See <i>destination identifier</i> .
<b>destination identifier</b>	A 3-byte field in a Fibre Channel frame header that indicates the targeted destination (address identifier of the device N_Port) of the transmitted frame.
<b>director</b>	A redundant, highly-available Fibre Channel switch with a high port count that provides any-to-any port connectivity between devices (nodes) connected to a switched fabric. A director transmits data frames between nodes in accordance with the address information provided in the associated frame headers. Directors are well suited

for use in enterprise computing environments. *Contrast with [fabric switch](#).*

**DNS** See [domain name system](#).

**DNS server** For Internet and TCP/IP applications, a DNS server supplies name-to-address translation by mapping domain names to Internet addresses.

**domain** (1) A group of devices (nodes) on a network that form an entity with resources under common control. For example, a domain can be a group of servers connected and named to simplify network administration and security. (2) For TCP/IP applications, the naming system used in a hierarchical network. (3) A Fibre Channel term describing the most significant byte in the N\_Port identifier of a Fibre Channel device.

**domain ID** A number that uniquely identifies a director or switch in a multswitch fabric. A unique domain ID is automatically allocated to each director or switch by the fabric's principal switch. *See also [preferred domain ID](#).*

**domain name system** The online distributed database system used by the Internet to map names to IP addresses. DNS servers connected to the Internet implement a hierarchical name space that allows sites freedom in assigning machine names and addresses. DNS also supports separate mappings between mail destinations and IP addresses.

## E

**E\_D\_TOV** See [error-detect time-out value](#).

**EFC Audit Log** A log that summarizing actions (audit trail) performed through the EFC Manager application. *Contrast with [Audit Log](#).*

**EFC Event Log** A log recorded at the EFC Manager application that displays a history of events or errors recorded by the EFC Management Services application. *Contrast with [Event Log](#).*

**EFCM** See [Enterprise Fabric Connectivity Management](#).



<b>EFCM Lite application</b>	The EFCM Lite application bundles the EFC Manager application, director or switch-specific Element Manager application, and Cluster Manager application on a CD-ROM for installation on a customer-supplied server. EFCM Lite is functionally equivalent to standard EFCM applications on a management server, except EFCM Lite does not support the call-home or automatic CD drive back up features.
<b>EFC Management Services application</b>	A user-transparent application that provides product independent services to the EFC Manager application. The application runs only on the management server and cannot be downloaded from the server to remote workstations.
<b>EFC Manager application</b>	An application providing the system management framework and user interface for managing McDATA directors and switches. The EFC Manager application runs locally on the management server and can be downloaded to remote user workstations. <i>See also <a href="#">Cluster Manager application</a> and <a href="#">Element Manager application</a>.</i>
<b>electrostatic discharge</b>	The inadvertent and undesirable discharge of static electricity that can damage or degrade electronic circuitry or components.
<b>Element Manager application</b>	An application providing the management and graphical user interface for a specific McDATA director and switch. Each managed product (director or switch) requires an instance of the Element Manager application. Each instance is opened from the EFC Manager application. The application runs locally on the management server and can be downloaded to remote user workstations. Formerly Product Manager application. <i>See also <a href="#">Cluster Manager application</a> and <a href="#">EFC Manager application</a>.</i>
<b>enterprise</b>	A series of computers, storage devices, and peripherals deployed in a high-volume and multi-user environment, and that collectively serves the needs of an entire business organization rather than a single user, department, or specialized application.
<b>Enterprise Fabric Connectivity Management</b>	A management scheme for McDATA directors and switches that includes the management server, EFC Management Services application, EFC Manager application, all director and switch-specific Element Manager applications, and the Cluster Manager application.
<b>Enterprise Systems Architecture</b>	A computer architecture introduced by IBM in 1988 as ESA/370. The architecture added access registers to improve virtual memory management and increase storage from 2 gigabyte to 6 terabytes. The architecture was enhanced with the introduction of ESA/390 in 1990.

**Enterprise Systems Connection** An IBM architecture, technology, and set of products and services introduced in 1990 that provides a dynamically-connected computing environment using fiber-optic cables as the data transmission medium. *See also* [Fibre Connection](#).

**E\_Port** *See* [expansion port](#).

**error-detect time-out value** The user-configured minimum time that a director or switch port waits for Fibre Channel sequence completion before declaring an error and initiating the recovery process.

**ESA** *See* [Enterprise Systems Architecture](#).

**ESCON** *See* [Enterprise Systems Connection](#).

**ESD** *See* [electrostatic discharge](#).

**Ethernet** A widely-implemented 10 or 100-Mbps LAN protocol that uses a bus or star topology based on the IEEE 802.3 standard. The protocol provides carrier-sense multiple access, and resolves signal contention using collision detection and transmission.

**event code** A three-digit number that identifies an event that occurred at a director, switch, or the management server. Event codes provide general system information or failure information. Fault isolation for McDATA products is event code driven.

**Event Log** A log recorded at the Element Manager application that displays a history of director or switch events, such as degraded operation, FRU failures, FRU removals and replacements, and link incidents. *Contrast with* [EFC Event Log](#).

**expansion port** In Fibre Channel protocol, a director or fabric switch port that connects to another director or switch E\_Port to form an ISL. *See also* [bridge port](#).

## F

**Fabric Log** A log recorded at the EFC Manager application that displays the time and nature of changes made to a managed fabric, such as a switch added or removed, ISL added or removed, fabric renamed or persisted, or zone set activated.

<b>fabric login</b>	The fabric login (FLOGI) command is initiated by a fabric-attached node port (N_Port) and establishes the operating parameters and topology required for fabric login. The command is accepted by a fabric port (F_Port).
<b>fabric loop port</b>	In Fibre Channel protocol, a switch port with arbitrated loop capability that communicates with a node loop port (NL_Port) of an attached FC-AL device. <i>See also</i> <a href="#">node loop port</a> , <i>contrast with</i> <a href="#">hub port</a> .
<b>fabric port</b>	In Fibre Channel protocol, a switch port that communicates with a node port (N_Port) of an attached Fibre Channel device. <i>See also</i> <a href="#">node port</a> .
<b>fabric switch</b>	A highly-available Fibre Channel switch with a low port count that provides any-to-any port connectivity between devices (nodes) connected to a switched fabric. A fabric switch transmits data frames between nodes in accordance with the address information provided in the associated frame headers. Fabric switches are well suited for use in workgroup or departmental computing environments. <i>Contrast with</i> <a href="#">director</a> .
<b>failover</b>	Automatic and nondisruptive transition of operation from an active FRU that failed to a functional backup FRU.
<b>FC-0</b>	The Fibre Channel layer that describes the physical link between two ports, including the transmission medium, transmitter and receiver circuitry, and interfaces.
<b>FC-1</b>	The Fibre Channel layer that defines the 8B/10B encoding, decoding, and transmission protocol.
<b>FC-2</b>	The Fibre Channel layer that specifies the signaling protocol, rules, and mechanisms required to transfer data blocks. This layer is complex and provides different classes of service, packetization, sequencing, error detection, segmentation, and reassembly of transmitted data.
<b>FC-3</b>	The Fibre Channel layer that provides a set of services common across multiple node ports (N_Ports) of a Fibre Channel node. The services are not commonly used and are essentially reserved for Fibre Channel architecture expansion.
<b>FC-4</b>	The Fibre Channel layer that provides mapping of Fibre Channel capabilities to upper level protocols (ULPs), including IP and SCSI.

<b>FC-AL</b>	Acronym for <i>Fibre Channel arbitrated loop</i> . Synonymous with <a href="#">arbitrated loop</a> .
<b>FC-PH</b>	See <a href="#">Fibre Channel Physical and Signaling Interface</a> .
<b>feature enablement key</b>	After purchasing a an additional product feature, McDATA provides a unique feature enablement key to the customer. A feature key is a case-sensitive alphanumeric string consisting of dashes, uppercase characters, and lowercase characters.
<b>fiber optics</b>	The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic. A single optical fiber or a nonspatially aligned fiber bundle is used for each information channel.
<b>fibre</b>	A generic Fibre Channel term used to describe transmission media types specified in the FC-PH standard, such as optical fiber, copper twisted pair, or copper coaxial cable.
<b>Fibre Channel</b>	An integrated set of ANSI standards that defines specific protocols for flexible information transfer. Logically, Fibre channel is a point-to-point serial data channel structured for high performance.
<b>Fibre Channel Physical and Signaling Interface</b>	An ANSI document that specifies the FC-0 (physical signaling), FC-1 (data encoding), and FC-2 (frame construct) layers of the Fibre Channel protocol.
<b>Fibre Channel Standard</b>	An ANSI standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.
<b>Fibre Connection</b>	An IBM architecture, technology, and set of products and services introduced in 1999 and based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance. FICON is the successor to ESCON, but is designed to coexist with ESCON technology. See also <a href="#">Enterprise Systems Connection</a> .
<b>fibre port module card</b>	A printed circuit board (Intrepid 6064 Director only) that provides four port connections that support 1.0625 Gbps Fibre Channel

communication. Port connectivity is provided through SFP optical transceivers. *Contrast with [universal port module card](#) and [10 Gbps port module card](#).*

**fibre shortest path first** A standard Dijkstra's networking algorithm that calculates to optimum path between switches in a Fibre Channel fabric. The FSPF algorithm is applied through the optional open trunking feature.

**FICON** See [Fibre Connection](#).

**FICON management server** An optional feature that enables inband management and host control of a director or switch through a server attached to a product port. The server communicates with the product through a FICON channel. *Contrast with [open-systems management server](#).*

**field-replaceable unit** An assembly removed and replaced in its entirety (on site) when any assembly components fails.

**FLOGI** See [fabric login](#).

**FL\_Port** See [fabric loop port](#).

**FPM card** See [fibre port module card](#).

**F\_Port** See [fabric port](#).

**FRU** See [field-replaceable unit](#).

**FSPF** See [fibre shortest path first](#).

**full-duplex** The capability to simultaneously communicate in both directions over a single connection, with flow control. *Synonymous with [bidirectional](#), contrast with [half-duplex](#).*

## G

**gateway address** For TCP/IP applications, the address of a router to which a device sends frames destined for addresses not on the same physical network as the sending device. The hexadecimal format for a gateway address is XXX.XXX.XXX.XXX.

**Gb** See [gigabit](#).

<b>GB</b>	See <i>gigabyte</i> .
<b>GBIC</b>	See <i>gigabit interface converter</i> .
<b>Gbps</b>	Acronym for gigabits per second. Also written as Gb/sec.
<b>generic port</b>	In Fibre Channel protocol, a director or switch port that functions as a fabric port (F_Port), fabric loop port (FL_Port), or expansion port (E_Port), depending on the port to which it connects. See also <i>fabric port</i> , <i>fabric loop port</i> , or <i>expansion port</i> .
<b>generic port module card</b>	A printed circuit board (ED-5000 Director only) that provides four port connections that support 1.0625 Gbps Fibre Channel communication. Port connectivity is provided through SC duplex optical transceivers. Contrast with <i>fibre port module card</i> and <i>universal port module card</i> .
<b>GHz</b>	See <i>gigahertz</i> .
<b>gigabit</b>	A unit of measure for data storage, equal to 134,217,728 bytes. A gigabit is generally approximated as one eighth of a gigabyte.
<b>gigabit interface converter</b>	A removable port connector (serial DB9, serial HSSDC, or fiber-optic) that converts an electrical data stream to an optical or amplified electrical data stream. GBICs provide port connectivity for the ES-1000 switch. Contrast with <i>SC duplex connector</i> and <i>small form factor pluggable transceiver</i> .
<b>gigabyte</b>	A unit of measure for data storage, equal to 1,073,741,824 bytes. A gigabyte is generally approximated as one billion bytes.
<b>gigahertz</b>	One billion cycles per second (Hertz).
<b>GLS card</b>	A G_Port, Longwave laser, Singlemode fiber variant of an ED-5000 Director GPM card. The card provides four longwave laser port connections. Contrast with <i>GSM card</i> and <i>GXX card</i> .
<b>GPM card</b>	See <i>generic port module card</i> .
<b>G_Port</b>	See <i>generic port</i> .
<b>graphical user interface</b>	A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen.

**GSM card** A G\_Port, Shortwave laser, Multimode fiber variant of an ED-5000 Director GPM card. The card provides four shortwave laser port connections. *Contrast with [GLS card](#) and [GXX card](#).*

**GUI** See *[graphical user interface](#)*.

**GXX card** A G\_Port, miXed laser, miXed fiber variant of an ED-5000 Director GPM card. The card provides three shortwave laser port connections and one longwave laser port connection. *Contrast with [GLS card](#) and [GSM card](#).*

## H

**half-duplex** The capability to communicate in both directions over a single connection, but not simultaneously (except for link control frames). *Contrast with [full-duplex](#).*

**Hardware Log** A log recorded at the Element Manager application that displays a history of FRU removals and replacements (insertions) for a director or switch.

**HBA** See *[host bus adapter](#)*.

**hexadecimal** A computer numbering system with base of sixteen. Valid numbers use the digits 0 through 9 and characters A through F.

**high availability** A director and switch performance feature characterized by component redundancy and the ability to perform concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

**high speed serial data connector** A 20-pin serial connector type that provides connectivity to an ES-1000 Switch GBIC. *Contrast with [DB-9 connector](#).*

**host bus adapter** A logic card that provides a link between a server and storage subsystem, and that integrates the operating systems and I/O protocols of both devices to ensure interoperability.

**H\_Port** See *[hub port](#)*.

**HSSDC** See *[high speed serial data connector](#)*.

**hub** A non intelligent device that connects Ethernet or Fibre Channel nodes into a logical loop by using a physical star topology.

**hub port** An arbitrated loop port that provides FC-AL device connectivity to the ES-1000 Switch. H\_Ports are not assigned port addresses and provide physical connectivity only. *Contrast with [fabric loop port](#).*

## I

**IML** See [initial machine load](#).

**inband management** Management of a director or switch through a Fibre Channel or FICON port connection to a management server. *Contrast with [out-of-band management](#).*

**initial machine load** A software operation that reloads director or switch firmware and resets the Ethernet LAN interface. An IML is typically performed by pressing the **IML** button at the director or switch front panel. An IML is functionally equivalent to an IPL.

**initial program load** A software operation that reloads director or switch firmware and resets the Ethernet LAN interface. An IPL is typically performed through a menu option at the director or switch Element Manager application. An IPL is functionally equivalent to an IML.

**Internet protocol address** A unique string of numbers (in the format XXX.XXX.XXX.XXX) that identifies a device on a TCP/IP network.

**interswitch link** A physical expansion port (E\_Port) connection between two fabric elements (directors or switches) in a multiswitch fabric.

**IP address** See [Internet protocol address](#).

**IPL** See [initial program load](#).

**ISL** See [interswitch link](#).



**K****Kb** See *kilobit*.**KB** See *kilobyte*.**kilobit** A unit of measure for data storage, equal to 1,024 bits. A kilobit is generally approximated as one thousand bits.**kilobyte** A unit of measure for data storage, equal to 1,024 bytes. A kilobyte is generally approximated as one thousand bytes.**L****LAN** See *local area network*.**laser** Acronym for *light amplification by stimulated emission of radiation*. A device that produces a powerful, narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.**latency** For Fibre Channel applications, the time elapsed between receipt of a data frame at a switch's incoming F\_Port to retransmission of the data through the switch's outgoing F\_Port to a destination N\_Port.**LED** See *light-emitting diode*.**light-emitting diode** A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on director or switch front bezels and FRUs to provide visual status indications.**LIN** See *link incident*.**link incident** The interruption of traffic on a Fibre Channel link due to loss of light or other malfunction.**Link Incident Log** A log recorded at the Element Manager application that displays a history of Fibre Channel link incidents (with associated port numbers) for a director or switch.**LIP sequence** See *loop initialization primitive sequence*.

**local area network** A communication system that links computers in a network through a wiring-based cable scheme. LANs connect servers, storage devices, and printers together to allow users to communicate and share resources. LAN devices are linked in a localized geographical area (for example, a building or campus), and are typically user-owned and do not run over leased lines. *Contrast with [metropolitan area network](#), [storage area network](#), and [wide area network](#).*

**logical port address** The address used to specify port connectivity parameters when a director or switch is set to operate in S/390 mode.

**logical unit number** In systems network architecture, a LUN is a number assigned to each logical partition of a storage device. Each logical partition is uniquely identified in a SAN when the LUN combines with the WWN of the storage device's N\_Port.

**loop initialization primitive sequence** A transmitted LIP sequence enables initialization of a Fibre Channel arbitrated loop. An arbitrated loop must initialize prior to operation and when configuration changes are detected. Any FL\_Port with a valid AL\_PA can start loop initialization by entering the initializing state and transmitting a LIP sequence.

**LUN** See [logical unit number](#).

## M

**MAC address** See [media access control address](#).

**maintenance port** Connector on a director or switch whereby a PC running an ASCII terminal emulator can be connected for specialized maintenance support.

**MAN** See [metropolitan area network](#).

**management information base** The related set of software objects (variables) that a gateway running the SNMP management protocol maintains. A MIB defines variables needed by the SNMP protocol to monitor and control components in the network.

**management server** A rack-mounted processor shipped with a director or switch, and dedicated to running the EFC Manager application, Element

Manager application, and Cluster Manager application. Formerly EFC Server.

**Mb** See *megabit*.

**MB** See *megabyte*.

**Mbps** Acronym for megabits per second.

**MBps** Acronym for megabytes per second.

**media access control address** A MAC address is a unique hardware number of a device on a LAN or other network. The MAC address is used by the media access control sublayer of the TCP/IP data-link layer.

**megabit** A unit of measure for data storage, equal to 1,048,576 bits. A megabit is generally approximated as one million bits.

**megabyte** A unit of measure for data storage, equal to 1,048,576 bytes. A megabyte is generally approximated as one million bytes.

**message path controller card** A printed circuit board (ED-5000 Director only) that provides the mechanism for messages to be sent and received between director ports. The board also provides a system clock source and central control and distribution of clocks for MPC, G\_Port module (GPM), and central memory module (CMM) boards.

**metropolitan area network** A high-speed communication network designed to link together sites in a metropolitan or campus area, comprised of distances up to 100 kilometers. *Contrast with [local area network](#), [storage area network](#), and [wide area network](#).*

**MIB** See *management information base*.

**MPC card** See *message path controller card*.

**multimode optical fiber** A graded-index or step-index optical fiber that allows more than one mode (light path) to propagate. *Contrast with [singlemode optical fiber](#).*

## N

**name server** In Fibre Channel protocol, a server that allows N\_Ports to register information. This allows devices to obtain information about other fabric-attached devices by sending queries to the name server.

**nickname** An alternate name assigned with a WWN to a director, switch, or other device in a switched fabric.

**NL\_Port** See [node loop port](#).

**node** In Fibre Channel protocol, a device (server, storage device, or other peripheral) that is connected to a switched fabric.

**node loop port** In Fibre Channel protocol, a connectivity port on an FC-AL device. An NL\_Port communicates with a switched fabric through a director or switch fabric loop port (FL\_Port). See also [fabric loop port](#).

**node port** In Fibre Channel protocol, a connectivity port on a Fibre Channel device. An N\_Port communicates with a switched fabric through a director or switch fabric port (F\_Port). See also [fabric port](#).

**nondisruptive maintenance** See [concurrent maintenance](#).

**N\_Port** See [node port](#).

## O

**offline sequence** A Fibre Channel primitive sequence transmitted by a port to indicate it is going offline.

**OLS** See [offline sequence](#).

**open-systems interconnection** A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, and the implementation of a layer can be changed without affecting other layers.

<b>open-systems management server</b>	An optional feature that enables inband management and host control of a director or switch through an OSI server attached to a product port. <i>Contrast with <a href="#">FICON management server</a>.</i>
<b>open-systems mode</b>	The management mode used to specify director or switch port connectivity when the product is attached to other McDATA products or OSI-compliant devices as part of an open fabric. <i>Contrast with <a href="#">S/390 mode</a>.</i>
<b>Operating System/390</b>	An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex support, object-oriented programming, distributed computing environment, and open application interfaces.
<b>OS/390</b>	<i>See <a href="#">Operating System/390</a>.</i>
<b>OSI</b>	<i>See <a href="#">open-systems interconnection</a>.</i>
<b>out-of-band management</b>	Management of a director or switch through an Ethernet port connection to a management server. <i>Contrast with <a href="#">inband management</a>.</i>
<b>P</b>	
<b>persistent binding</b>	A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number.
<b>point-to-point</b>	One of three topologies offered by the Fibre Channel protocol. The topology is structured as a single, direct connection between two communication ports. <i>See also <a href="#">arbitrated loop</a> and <a href="#">switched fabric</a>.</i>
<b>POST</b>	<i>See <a href="#">power-on self-test</a>.</i>
<b>power-on self-test</b>	A series of self-diagnostic tests that run automatically when a device powers on.
<b>preferred domain ID</b>	The domain ID that a director or switch requests from a fabric principal switch. If the preferred value is in use, the principal switch assigns a different value. <i>See also <a href="#">domain ID</a>.</i>

<b>principal switch</b>	In a multiswitch fabric, the switch that allocates domain IDs to itself and all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.
<b>private device</b>	An arbitrated loop device that cannot transmit a FLOGI command to a switch or director, nor communicate with fabric-attached devices. <i>Contrast with <a href="#">public device</a>.</i>
<b>private loop</b>	A private arbitrated loop is not connected to a switched fabric. All devices attached to the loop can only communicate with each other. <i>Contrast with <a href="#">public loop</a>.</i>
<b>Product Status Log</b>	A log recorded at the EFC Manager application that displays an entry when the status of a director or switch changes. The log reflects the previous status and current status of a managed product, and indicates the instance of a Element Manager application that should be opened to investigate a problem.
<b>public device</b>	An arbitrated loop device that can transmit a FLOGI command a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. <i>Contrast with <a href="#">private device</a>.</i>
<b>public loop</b>	A public arbitrated loop is connected to a switched fabric. All devices attached to the loop can communicate with each other, and public devices attached to the loop can communicate with fabric-attached devices. <i>Contrast with <a href="#">private loop</a>.</i>
<b>R</b>	
<b>radio frequency interference</b>	Electromagnetic radiation emitted by electrical circuits during normal operation, which causes unwanted signals (interference or noise) to be induced in other circuits.
<b>R_A_TOV</b>	See <a href="#">resource allocation time-out value</a> .
<b>redundancy</b>	Performance characteristic of a system or product whose integral components are backed up by identical components to which operations automatically failover after component failure. Redundancy is a vital characteristic of high-availability computer systems and networks.

**remote notification** The process by which a system informs remote users and workstations of certain classes of events that occur. Call-home notification, e-mail notification and configuration of SNMP trap recipients are examples of remote notification programs implemented on directors and switches.

**resource allocation time-out value** The user-configured minimum time that a director or switch port waits for Fibre Channel frame delivery through a switched fabric before initiating the recovery process.

**RFI** See *radio frequency interference*.

**RS-232** The Electronic Industry Association recommended specification for asynchronous serial interfaces between computers and other communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals.

## S

**S/390 mode** The management mode used to specify director or switch port connectivity when the product is attached to an IBM System/390 (generation 5 or later) or zSeries 900 Parallel Enterprise Server with one or more FICON channel cards installed. *Contrast with open-systems mode.*

**SAN** See *storage area network*.

**SANpilot interface** The SANpilot interface provides a GUI similar to the Element Manager application, and supports director or switch configuration, statistics monitoring, and basic operation. With director or switch firmware installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the director or switch through the interface.

**SBAR** See *serial crossbar assembly*.

**scalable** The ability of a system to adapt to increased demands. A scalable network could start with a few nodes but easily expand to thousands of nodes.

**SC duplex connector** An optical fiber connector that terminates jumper cables in one housing and provides physical attachment to a subscriber connector

	(SC) duplex receptacle. SC duplex connectors provide optical port connectivity for the ED-5000 Director and ES-1000 switch. <i>Contrast with <a href="#">gigabit interface converter</a> and <a href="#">small form factor pluggable transceiver</a>.</i>
<b>serial crossbar assembly</b>	A printed circuit board (Intrepid-series directors only) that provides Fibre Channel frame transmission from any director port to any other director port. Connections are established without software intervention.
<b>Session Log</b>	A log recorded at the EFC Manager application that displays a session (login and logout) history for the management server, including the date and time, user name, and network address of each session.
<b>SFP transceiver</b>	See <a href="#">small form factor pluggable transceiver</a> .
<b>shared mode</b>	When an ES-1000 Switch is set to shared mode, the switch acts as a hub that implements arbitrated loop topology. An attached device communicates with another device using the full switch bandwidth. During frame transmission between the device pair, no other switch ports or attached devices can communicate. <i>Contrast with <a href="#">switched mode</a>.</i>
<b>simple mail transfer protocol</b>	The TCP/IP standard protocol for transferring electronic mail messages from one machine to another. SMTP specifies how mail systems interact and the format of control messages they exchange to transfer mail.
<b>simple network management protocol</b>	A protocol defined for TCP/IP-based network management, widely accepted as the standard for LAN network management. SNMP consists of three parts: structure of management information (SMI), a management information base (MIB), and the protocol itself. The SMI and MIB define and store the set of managed entities; the protocol conveys information to and from these entities.
<b>singlemode optical fiber</b>	An optical fiber that allows one wavelength-dependent mode (light path) to propagate. <i>Contrast with <a href="#">multimode optical fiber</a>.</i>
<b>small form factor pluggable transceiver</b>	A laser-driven small form factor optical transceiver used for a wide range of networking applications requiring high data rates (usually 1 and 2 Gbps). SFP transceivers provide port connectivity for Intrepid-series directors and Sphereon-series switches. <i>Contrast with <a href="#">gigabit interface converter</a> and <a href="#">SC duplex connector</a>.</i>



**SMTP** See *simple mail transfer protocol*.

**SNMP** See *simple network management protocol*.

**SNMP community** The relationship between an SNMP agent and a set of SNMP managers that define authentication, access control, and proxy characteristics. An SNMP community is specified by a name that the agent software recognizes as a valid source for SNMP requests.

**storage area network** A dedicated, high-performance data communication network that establishes a direct connection between servers and storage devices. SANs are typically connected through Fibre Channel directors and fabric switches, and allows resources to be effectively shared and consolidated. *Contrast with* *local area network*, *metropolitan area network*, and *wide area network*.

**subnet mask** A subnet mask is used by a computer to determine if another computer is located on a local or remote network. The subnet mask depends on the class of network to which the computer is connecting. The mask indicates the digits to search in a longer network address, and allows a router to avoid handling the entire address. Typically, a subnet represents all devices configured at one location, building, or on the same LAN.

**switched fabric** One of three topologies offered by the Fibre Channel protocol. The topology is structured as a network of one or more interconnected switch elements. Each element connects device N\_Ports and is capable of routing (switching) Fibre Channel frames, using destination ID information accompanying data frames. *See also* *point-to-point* and *switched fabric*.

**switched mode** When an ES-1000 Switch is set to switched mode, the switch bypasses loop arbitration and enables frame transmission through multiple, logical connected device pairs. All connected device pairs share the switch bandwidth. *Contrast with* *shared mode*.

**switch priority** A value configured for each switch in a fabric that determines the relative likelihood of the switch becoming the fabric principal switch. A low value indicates a high likelihood of becoming the principal switch.

**T**

**TCP** See *transmission control protocol*.

**TCP/IP** See *transmission control protocol/Internet protocol*.

**Telnet** The user command and underlying TCP/IP protocol for remote terminal access and connection over a network.

**Threshold Alert Log** A log recorded at the Element Manager application that displays a history of threshold alert notifications for a director or switch, including the date and time an alert occurred.

**transmission control protocol** The TCP/IP transport layer, widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections.

**transmission control protocol/Internet protocol** A layered set of protocols (network and transport) that allows sharing of applications among devices in a high-speed LAN communication environment.

**trap** An unsolicited notification of an event originating from an SNMP-managed device and directed to an SNMP network management station.

**trap recipient** In SNMP, a network management station that receives messages for configured events that occur at a managed director or switch.

**U**

**UDP** See *user datagram protocol*.

**ULP** See *upper level protocol*.

**uniform resource locator** The address (specified as a name or IP address) of a document or other resource available on the Internet.

**uninterruptable power supply** A buffer between public utility power or other power source, and a system that requires precise, uninterrupted power.

<b>universal port module card</b>	A printed circuit board (Intrepid-series directors only) that provides four port connections that support 1.0625 or 2.125 Gbps Fibre Channel communication. Port connectivity is provided through SFP optical transceivers. <i>Contrast with <a href="#">fibre port module card</a> and <a href="#">10 Gbps port module card</a>.</i>
<b>UPM</b>	<i>See <a href="#">universal port module card</a>.</i>
<b>upper level protocol</b>	A protocol that maps to and runs on top of the Fibre Channel through the FC-4 layer. Examples of upper level protocols include Internet protocol (IP) and small computer system interface (SCSI).
<b>UPS</b>	<i>See <a href="#">uninterruptable power supply</a>.</i>
<b>URL</b>	<i>See <a href="#">uniform resource locator</a>.</i>
<b>user datagram protocol</b>	A connectionless protocol that runs on top of IP networks. UDP offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP is primarily used for broadcasting messages over an entire network.
<b>V</b>	
<b>vital product data</b>	System-level data stored by FRUs in electrically erasable programmable read-only memory. VPD identifies the manufacturer and includes the FRU part number and serial number.
<b>VPD</b>	<i>See <a href="#">vital product data</a>.</i>
<b>W</b>	
<b>WAN</b>	<i>See <a href="#">wide area network</a>.</i>
<b>well-known address</b>	A set of address identifiers defined in the Fibre Channel Physical and Signaling Interface specification that access global server functions such as a login server, management server, or name server.

**wide area network** A network that covers a larger geographical area than a LAN and where telecommunications links are typically leased through a common carrier. *Contrast with [local area network](#), [metropolitan area network](#), and [storage area network](#).*

**world-wide name** An eight-byte string that uniquely identifies a Fibre Channel entity such as a port, node, director, switch, or fabric.

**WWN** *See [world-wide name](#).*

## X

**XFP transceiver** *See [10 Gbps form factor pluggable transceiver](#).*

**XPM** *See [10 Gbps port module card](#).*

## Z

**zone** A set of logically-partitioned devices. Zone members can recognize each other and communicate through switched port-to-port connections. Nonmember devices cannot. *See also [active zone set](#), [zone set](#), and [zoning](#).*

**zone member** A device (server, storage device, or other peripheral) included in a zone. Zone members are identified by port number or WWN.

**zone set** A group of zones activated or deactivated as one entity. *See also [active zone set](#) and [zone](#).*

**zoning** The partitioning of devices attached to a director or switch into restricted access groups called zones. Devices are commonly zoned for security, to differentiate operating systems, or because of common functionality.

## Numerics

- 10 Gbps form factor pluggable optical transceiver
  - See XFP optical transceiver
- 10/100 BaseT ethernet hub [1-1](#)
- 10/100 Mbps
  - ethernet port [1-6](#)

## A

- AC module [1-11](#)
  - removing and replacing [5-24](#)
- AC system harness [1-11](#)
- acoustical noise, director [C-2](#)
- airflow clearances, director [C-1](#)
- allen wrench, caution [1-15](#)
- altitude
  - operating environment [C-2](#)
  - shipping and storage environment [C-2](#)
- angular velocity, of fans [1-11](#)
- asynchronous RS-232
  - null modem cable [1-17](#)
- audit logs
  - director [4-6](#)
  - EFC manager [4-4](#)

## B

- backing up, director configuration file [4-75](#)
- backplane [1-12](#)
  - removing and replacing [5-35](#)
- bb\_credit
  - configure [2-55](#)
  - extended distance buffering [2-64](#)
- beaconing

- LED [1-5](#)
- bezel [1-5](#)
- binding
  - fabric
    - configure [2-106](#)
    - description [2-106](#)
  - port
    - configure [2-66, 2-100](#)
    - description [2-100](#)
  - switch
    - configure [2-101](#)
    - description [2-101](#)
    - disable [2-60, 2-101](#)
    - enable [2-60, 2-101](#)
    - online state requirements [2-59](#)
- blocking
  - port [4-46, 4-49](#)
  - UPM card [4-47](#)
  - XPM card [4-47](#)
- brackets, mounting, installing [2-13](#)

## C

- cabling fibre channel ports [2-113](#)
- call-home notification
  - configure [2-38](#)
  - enabling [2-76](#)
- caution statements, list of [-xxviii](#)
- CFR, laser compliance [-xxvi, 1-7](#)
- channel wrap test, procedure [4-37](#)
- class 1 laser products [-xxvi](#)
- class 1 laser transceivers [1-7](#)
- class F processing [1-6](#)
- cleaning fiber-optic components [4-50](#)

- clear
    - port statistics [4-24](#)
  - clear system error light function [1-5](#)
  - clearances, Fabriccenter cabinet [C-3](#)
  - Code of Federal Regulations [1-7](#)
    - laser compliance [-xxvi](#)
  - code page table [2-48](#)
  - command line interface
    - disable at SANpilot [2-97](#)
    - enable at SANpilot [2-97](#)
  - community name field [2-67](#)
  - COMn properties dialog box [2-16](#)
  - concurrent FRUs table [5-5](#)
  - configuration changes, audit log [4-6](#)
  - configuration data
    - backing up [2-78](#)
    - managing [4-74](#)
  - configure
    - bb\_credit [2-55](#)
    - call-home feature [2-38](#)
    - director date and time [2-87](#)
    - director identification [2-51, 2-86](#)
    - director network information [2-93](#)
    - director operating parameters [2-88](#)
    - director, from SANpilot [2-80](#)
    - e\_d\_tov [2-56](#)
    - e-mail notification [2-73](#)
    - ethernet events [2-75](#)
    - fabric binding [2-106](#)
    - fabric parameters [2-91](#)
    - feature key [2-45, 2-111](#)
    - FMS [2-47](#)
    - management server DNS domain name [2-25](#)
    - management server IP address [2-22](#)
    - management server name [2-25](#)
    - management server password [2-22](#)
    - management server subnet mask [2-22](#)
    - OpenTrunking [2-71, 2-108](#)
    - operating mode [2-52](#)
    - operating parameters [2-53, 2-55](#)
    - OSMS [2-46, 2-98](#)
    - port binding [2-66, 2-100](#)
    - ports [2-63, 2-84](#)
    - r\_a\_tov [2-55](#)
    - SNMP [2-95](#)
    - SNMP trap message recipients [2-66](#)
    - switch binding [2-101](#)
    - threshold alerts [2-67](#)
    - users dialog box [2-40](#)
    - Windows 2000 users [2-30](#)
    - zone sets [2-114](#)
    - zones [2-113](#)
  - connect to dialog box [2-16](#)
  - connecting, director to fabric [2-118](#)
  - connection description dialog box [2-16](#)
  - counter [4-25](#)
  - CTP card
    - description [1-5](#)
    - event codes [B-36](#)
    - failover [1-6](#)
    - firmware versions [4-55](#)
    - firmware, managing [4-55](#)
    - FLASH memory [4-39](#)
    - IML button [1-5](#)
    - LEDs [1-7](#)
    - MAP [3-74](#)
    - NV-RAM, backing up [4-74](#)
    - removing and replacing [5-6](#)
    - reset button [1-5](#)
  - customer checklist for fault isolation [3-9](#)
  - customer-supplied equipment rack [2-3](#)
- ## D
- danger statements, list of [-xxviii](#)
  - data collection procedure
    - management server [4-40](#)
    - SANpilot [4-41](#)
  - date and time
    - setting [2-50, 2-87](#)
    - synchronizing [2-51](#)
  - default
    - DNS server IP address [2-39](#)
    - EFC Manager password [4-89](#)
    - EFC manager password [2-80](#)
    - EFC Manager user name [4-89](#)
    - EFC manager user name [2-80](#)
    - factory, resetting [4-77](#)
    - gateway address [2-1](#)
    - IP address [2-1](#)
    - password [2-1](#)
    - resetting [4-77](#)
    - SAN management application password [E-7](#)
    - SAN management application user name [E-7](#)

- SANpilot password 2-83
  - SANpilot user name 2-83
  - subnet mask 2-1
  - switch priority 2-56, 3-115
  - TightVNC password 2-26, 2-80, 4-88, E-5
  - Windows 2000 password 2-27, 2-80, 4-89, E-6
  - Windows 2000 user name 2-27, 2-80, 4-89, E-6
  - definition
    - wraps 4-25
  - diagnostics
    - MAPs 3-1
    - port diagnostics 4-13
  - dimensions, director C-1
  - director
    - AC module 1-11
    - acoustical noise C-2
    - airflow clearances C-1
    - audit log 4-6
    - CTP card 1-6
    - dimensions C-1
    - displaying information 4-30
    - element manager
      - messages A-1
    - ethernet link, MAP 3-56
    - event codes B-1
    - event log 4-6, B-1
    - fabric log 4-6
    - fabric, connecting to 2-118
    - fan module 1-11
    - fault isolation 3-9
    - features
      - error-detection 1-12
      - reporting 1-12
      - serviceability 1-12
    - general description 1-1
    - heat dissipation C-1
    - identification, configure 2-51
    - illustrated parts breakdown 6-1
    - IML 1-5, 4-53
    - installation tasks, summary 2-3
    - IPL 4-53, 4-54
    - management, overview 1-18
    - MAPs 3-1
    - maximum inclination C-2
    - operating environment C-2
    - operating mode, configure 2-52
    - physical characteristics C-1
    - ports
      - blocking or unblocking 4-46
      - port list view 4-15
    - power requirements C-1
    - power supply 1-10
    - power-off procedure 4-52
    - power-on procedure 4-51
    - product status log 4-5
    - rack-mount, installing 2-13
    - reset 1-5, 4-53, 4-55
    - SANpilot
      - configure from 2-80
    - SBAR assembly 1-11
    - setting online or offline 4-43
    - shipping environment C-2
    - specifications C-1
    - storage environment C-2
    - tools supplied 1-15
    - unpacking, inspecting, installing 2-12
    - weight C-1
  - door key 1-16
  - download firmware
    - from file center 4-67
    - through SANpilot interface 4-72
  - DRAM 4-39
- ## E
- e\_d\_tov 2-92
    - configure 2-56
  - E\_Port
    - configuring 2-63
  - e\_port
    - configure 2-84
  - e\_port segmentation
    - link incident log 4-9
    - MAP 3-104
    - reasons for 4-22
  - EFC manager
    - audit log 4-4
    - default password 2-80
    - default user name 2-80
    - director identification, configure 2-51
    - event log 4-4
    - login dialog box 2-39
    - logs, list of 4-3

- EFC Manager application
    - default password [4-89](#)
    - default user name [4-89](#)
    - See EFC manager
  - EFC server
    - See management server
  - electrostatic discharge
    - See ESD
  - element manager
    - configure [2-49](#)
    - logs, list of [4-3](#)
    - messages [A-1](#)
    - performance view [4-16](#)
    - port list view [4-15](#)
    - SNMP [1-18](#)
  - e-mail notification
    - configure [2-73](#)
  - embedded port subsystem [1-6](#)
  - embedded web server interface
    - See SANpilot
  - enable
    - fabric binding [2-106](#)
    - port binding [2-66](#)
    - switch binding [2-101](#)
  - enterprise fabric mode
    - enable at SANpilot [2-107](#)
  - EP subsystem [1-6](#)
  - equipment cabinet, service clearances [C-3](#)
  - equipment rack, customer-supplied [2-3](#)
  - error
    - statistics [4-27](#)
  - error-detection features, director [1-12](#)
  - ESD
    - FRUs
      - illustration [6-1](#)
      - removing and replacing [5-2](#)
    - grounding point
      - front [5-4](#)
    - information [5-3](#)
    - precautions [-xxix](#)
    - repair procedures, caution [4-2](#)
    - wrist strap [1-17](#)
  - ethernet
    - communication link, MAP [3-56](#)
    - events, configure at management server [2-75](#)
    - events, enable at management server [2-75](#)
  - ethernet hub
    - description [D-2](#)
    - installation tasks, summary [2-3](#)
    - unpacking, inspecting, installing [2-9](#)
    - verify operation [3-60](#)
  - European Norm, compliance [-xxvi](#)
  - event codes [B-1](#)
    - CTP card events [B-36](#)
    - fan module events [B-28](#)
    - power supply [B-24](#)
    - SBAR assembly [B-61](#)
    - system events [B-3](#)
    - thermal events [B-67](#)
    - UPM card [B-48](#)
    - XPM card [B-48](#)
  - event log
    - director [4-6](#)
    - EFC manager [4-4](#)
    - management server [B-1](#)
  - exception frame processing [1-6](#)
  - external loopback test [4-36](#)
- ## F
- F\_Port
    - configuring [2-63](#)
  - f\_port
    - configure [2-84](#)
  - fabric binding
    - configure [2-106](#)
    - description [2-106](#)
  - fabric log [4-6](#)
  - fabric logout, MAP [3-104](#)
  - fabric parameters
    - configure at SANpilot [2-91](#)
  - Fabriccenter cabinet [1-1, 2-3](#)
    - door key [1-16](#)
    - ethernet hub installation [2-9](#)
    - service clearances [C-3](#)
  - factory defaults, resetting [4-77](#)
  - failover, SBAR assembly [1-11](#)
  - fan module [1-11](#)
    - MAP [3-74](#)
    - removing and replacing [5-27](#)
  - fan module events, event codes [B-28](#)
  - fault isolation [3-1](#)
    - customer checklist [3-9](#)
    - logs [4-3](#)



- MAPs 3-1
  - FC fabric element MIB, version 1-14
  - FC-512 Fabriccenter cabinet 1-1
  - FCC, compliance -xxvii
  - FC-PH 4.3 1-1
  - feature keys
    - configure 2-45, 2-111
    - OSMS 2-111
  - Federal Communications Commission,
    - compliance -xxvii
  - fiber-optic
    - cleaning kit 1-18
    - components, cleaning 4-50
    - protective plug 1-16
    - transceivers, types of 1-9
  - Fibre Alliance MIB 1-14
  - fibre channel
    - link incidents, MAP 3-82
    - physical and signalling interface 1-1
    - ports, cabling 2-113
  - FICON 2-45
    - channel wrap tests
      - procedure 4-37
    - fibre channel
      - port address, swapping 4-16, 4-18
  - FMS, configure 2-47
    - management server 2-45
    - management server, configure 2-47
    - port channel wrapping, enabling and
      - disabling 4-16, 4-18
    - swapping ports, procedure 4-38
  - field-replaceable units
    - See FRUs
  - file center
    - download EFC Manager application 4-82
    - download firmware to browser PC 4-67
    - registration 2-120
  - firmware
    - add version to browser PC 4-67
    - adding version 4-56
    - determine version at SANpilot interface 4-66
    - determining version 4-56
    - download through SANpilot interface 4-72
    - download version from file center 4-67
    - downloading version 4-63
    - versions, managing 4-55
  - FL\_Port
    - configuring 2-63
  - FLASH memory 4-39
  - FMS
    - configure 2-47
  - frames
    - too short, error statistics 4-27
  - front bezel 1-5
  - front-accessible FRUs, parts list 6-3
  - FRUs
    - AC module 1-11
    - backplane 1-12
    - concurrent 5-5
    - CTP card 1-5
    - description 1-4
    - ESD precautions -xxix, 5-2
    - fan module 1-11
    - front access, illustration 1-4
    - front-accessible 6-2
      - parts list 6-3
    - illustrations 6-1
    - nonconcurrent 5-5
    - power supply 1-10
    - Power/System Power LED Assembly 1-5
    - rear access, illustration 1-5
    - rear-accessible 6-4, 6-7
      - parts list 6-5, 6-6, 6-8
    - removals and replacements, hardware log 4-8
    - removing and replacing 5-2
    - SBAR assembly 1-11
    - serial number, hardware log 4-8
    - UPM card 1-6
    - XPM card 1-6
  - full-volatility feature
    - description 4-40
- ## G
- g\_port
    - UPM card 1-7
    - XPM card 1-8
  - gateway address
    - change director address 2-93
    - default 2-1, 3-2, 4-2, 5-1
  - grounding point
    - front 5-4

**H**

hardware log 4-8  
 hardware view  
     displaying director information 4-30  
 heat dissipation, director C-1  
 hexagonal adapter 1-15  
 humidity  
     operating environment C-2  
     shipping and storage environment C-2  
 HyperTerminal 1-18, 3-65

**I**

identification  
     configure at SANpilot 2-86  
 illustrated parts breakdown 6-1  
 IML 1-5, 4-53  
 inclination, maximum, director C-2  
 initial program load, MAP 3-42  
 input filter 1-11  
 insistent domain ID 2-54, 2-90  
 installation options  
     desktop 2-3  
 installation requirements, verifying 2-8  
 installation task summary table 2-4  
 installation tasks  
     call-home feature, configure 2-38  
     configuration data, backing up 2-78  
     director  
         date and time, setting 2-50  
         EFC manager, configure to 2-42  
         element manager, configure 2-49  
         ethernet LAN, connecting 2-19  
         fabric, connecting 2-118  
         maintenance server communication, verifying 2-43  
         network information, configure 2-15  
         SANpilot, configure from 2-80  
         unpacking, inspecting, installing 2-12  
     ethernet hub, unpacking, inspecting, installing 2-9  
     feature key, configure 2-45  
     fibre channel ports, cabling 2-113  
     management server  
         date and time, setting 2-36  
         restore information, recording and verifying 2-39  
         unpacking, inspecting, installing 2-20  
         management server, configure 2-46  
         password, assigning 2-39  
         requirements, verifying 2-8  
         summary 2-3  
         Task 22 - Configure zoning (optional) 2-113  
         user names, assigning 2-39  
     installing software 4-82  
     internal loopback 4-34  
 International Electrotechnical Commission, compliance -xxvi  
 interop mode 2-92  
 interswitch link  
     MAP 3-104  
 Intrepid 6140 Director  
     See director  
 IP address  
     change director address 2-93  
     default 2-1, 3-2, 4-2, 5-1  
     DNS server default 2-39  
 IPL 4-53, 4-54  
     MAP 3-42  
 ISL  
     MAP 3-104

**L**  
 languages, code page table 2-48  
 laser transceivers 1-7  
 lasers, compliance statement -xxvi  
 LEDs  
     beaconing 1-5  
     CTP card 1-7  
     fan module 1-11  
     front bezel 1-5  
     POSTs 2-14  
     power supply 1-11  
     SBAR assembly 1-12  
     system error 1-5  
     UPM card 1-7, 4-13  
     XPM card 1-8, 4-13  
 LIN alerts 4-16  
 link incident alerts 4-16  
 link incident log  
     description 4-9  
 link incident, problem descriptions, list of 4-9  
 list

switch binding membership [2-102](#)

logic card, torque tool, caution [1-15](#)

logs

audit

director [4-6](#)

EFC manager [4-4](#)

event

director [4-6](#)

EFC manager [4-4](#)

fabric [4-6](#)

hardware [4-8](#)

link incident [4-9](#)

list of [4-3](#)

product status [4-5](#)

session [4-5](#)

loopback plug

multimode [1-16](#)

singlemode [1-16](#)

loopback test

external [4-32](#), [4-36](#)

internal [4-31](#), [4-34](#)

name server zoning, caution [4-33](#)

performing [4-30](#)

## M

maintenance analysis procedures

See MAPs

maintenance data, collecting [4-39](#)

management server

configure [2-46](#)

date and time, setting [2-36](#)

description [D-1](#)

director, verifying communication [2-43](#)

ethernet link, MAP [3-56](#)

event log [B-1](#)

fault isolation

MAP [3-9](#)

Fibre Alliance MIB [1-14](#)

firmware versions, storing [4-55](#)

inspecting [2-20](#)

installation tasks, summary [2-3](#)

installing [2-20](#)

restore information, recording and verifying  
[2-39](#)

restore procedure [E-2](#)

restore requirements [E-1](#)

session log [4-5](#)

specifications [D-2](#)

unpacking [2-20](#)

managing

configuration data [4-74](#)

director [1-18](#)

MAPs [3-1](#)

MAP 0000-Start Map [3-9](#)

MAP 0100-Power Distribution Analysis [3-33](#)

MAP 0200-POST Failure Analysis [3-42](#)

MAP 0300-Console Application Problem  
Determination [3-47](#)

MAP 0400-Loss of Console Communication  
[3-56](#)

MAP 0500-FRU Failure Analysis [3-74](#)

MAP 0600-Port Card Failure and Link  
Incident Analysis [3-82](#)

MAP 0700-Fabric, ISL, and Segmented Port  
Problem Determination [3-104](#)

MAP 0800-Console PC Problem  
Determination [3-121](#)

quick start [3-2](#)

summary table [3-2](#)

McDATA

home page

firmware versions [4-56](#)

warranty [-xxvii](#)

McDATA fabric 1.0 [2-56](#)

membership list

switch binding [2-102](#)

messages

element manager [A-1](#)

MIBs [1-14](#)

mode

McDATA fabric 1.0 [2-56](#)

open fabric 1.0 [2-57](#)

mounting brackets, installing [2-13](#)

multiswitch fabric

e\_port segmentation

reasons for [4-22](#)

## N

network address, product status log [4-5](#)

network information

configure director at SANpilot [2-93](#)

configure management server [2-22](#)

new product dialog box [2-42](#)  
 nonconcurrent FRUs table [5-5](#)  
 null modem cable [1-17](#)  
 NV-RAM, backing up [4-74](#)

## O

OFC class 1 laser transceivers [1-7](#)  
 offline state  
     set from SANpilot [4-45](#)  
 offline state, setting [4-44](#)  
 online state  
     set from SANpilot [4-45](#)  
 online state, setting [4-44](#)  
 open fabric 1.0 [2-57](#)  
 open systems management server  
     See OSMS  
 open systems mode  
     OSMS, configure [2-46](#)  
 OpenTrunking  
     configure at management server [2-71](#)  
     configure at SANpilot [2-108](#)  
 operating environment, director [C-2](#)  
 operating mode  
     configure [2-52](#)  
 operating parameters  
     configure at SANpilot [2-88](#)  
 operating parameters, configure [2-53](#), [2-55](#)  
 OSI server [2-46](#)  
 OSMS [2-45](#)  
     configure [2-46](#), [2-98](#)  
     feature key [2-111](#)

## P

part numbers  
     front-accessible FRUs [6-2](#)  
     rear-accessible FRUs [6-4](#), [6-7](#)  
 password  
     default [2-1](#), [3-2](#), [4-2](#), [5-1](#)  
     default EFC Manager [4-89](#)  
     default EFC manager [2-80](#)  
     default SAN management application [E-7](#)  
     default SANpilot [2-83](#)  
     default TightVNC [2-26](#), [2-80](#), [4-88](#), [E-5](#)  
     default Windows 2000 [2-27](#), [2-80](#), [4-89](#), [E-6](#)  
 performance statistics  
     Class 2 [4-18](#)

Class 3 [4-18](#)  
 error [4-18](#)  
 operational [4-20](#)  
 traffic [4-20](#)  
 physical characteristics, director [C-1](#)  
 planning tasks [2-8](#)  
     installation requirements, verifying [2-8](#)  
 port  
     clear statistics [4-24](#)  
 port binding  
     configure [2-66](#), [2-100](#)  
     description [2-100](#)  
 port card  
     external loopback test [4-32](#)  
     internal loopback test [4-31](#)  
     operational states [4-13](#)  
 port list view [4-15](#)  
 port loopback diagnostic tests, fiber-optic  
     loopback plug [1-16](#)  
 port operational states table [4-13](#)  
 port properties dialog box [4-16](#), [4-20](#)  
 port settings parameters [2-17](#)  
 ports  
     blocking [4-46](#)  
     configure at management server [2-63](#)  
     configure at SANpilot [2-84](#)  
     diagnostics, performing [4-13](#)  
     fibre channel, cabling [2-113](#)  
     operational states, list of [4-13](#)  
     performance statistics [4-24](#)  
     port properties [4-28](#)  
     port technology [4-22](#), [4-28](#)  
     unblocking [4-47](#)  
 POSTs  
     LEDs [2-14](#)  
     MAP [3-42](#)  
 power cords  
     illustrations [6-9](#)  
 power distribution system MAP [3-33](#)  
 power receptacles, illustrations [6-9](#)  
 power requirements, director [C-1](#)  
 power supply [1-10](#)  
     event codes [B-24](#)  
     LEDs [1-11](#)  
     removing and replacing [5-20](#)  
 Power/System Error LED assembly  
     removing and replacing [5-30](#)

power-off procedure [4-52](#)  
 power-on procedure [4-51](#)  
 power-on self-tests, MAP [3-42](#)  
 precautions  
     ESD [-xxix](#)  
     general [-xxix](#)  
 preferred domain ID [2-54](#), [2-89](#)  
 preventive maintenance, cleaning fiber-optic  
     components [4-50](#)  
 principal switch, configure [2-56](#)  
 principal switch, configuring [3-115](#)  
 procedural notes [4-2](#)  
 procedures  
     blocking ports [4-46](#)  
     data collection [4-39](#)  
     external loopback test [4-32](#)  
     FRU removal [5-2](#)  
     FRU replacement [5-2](#)  
     IML [4-53](#)  
     installing software [4-82](#)  
     internal loopback test [4-31](#)  
     IPL [4-54](#)  
     managing configuration data [4-74](#)  
     managing firmware versions [4-55](#)  
     MAPs [3-1](#)  
     power-off [4-52](#)  
     power-on [4-51](#)  
     reset [4-55](#)  
     setting offline [4-43](#)  
     setting online [4-43](#)  
     unblocking ports [4-47](#)  
     upgrading software [4-82](#)  
 ProComm Plus [1-18](#)  
 Product Manager  
     See element manager  
 product status log [4-5](#)  
 protective plug [1-16](#)  
 publications  
     related [-xxv](#)

## Q

quick start, MAPs [3-2](#)

## R

r\_a\_tov  
     configure [2-55](#)

rack-mount, installing [2-13](#)  
 radio frequency interference, compliance [-xxvii](#)  
 rear-accessible FRUs, parts list [6-5](#), [6-6](#), [6-8](#)  
 registered trademarks [-xxvi](#)  
 related publications [-xxv](#)  
 relative humidity  
     operating environment [C-2](#)  
     shipping and storage environment [C-2](#)  
 remove and replace procedures  
     See RRP's  
 repair procedures  
     IML, IPL, or reset the director repair  
         procedures  
         IML, IPL or reset the director [4-53](#)  
 repair procedures, notes [4-2](#)  
 reporting features, director [1-12](#)  
 rerouting delay [2-54](#), [2-90](#)  
 reset [1-5](#), [4-53](#)  
     configuration data from SANpilot interface  
         [4-80](#)  
 reset, director [4-55](#)  
 resetting  
     director configuration data [4-77](#)  
 restore  
     management server [E-2](#)  
 restoring  
     director configuration file [4-76](#)  
 RFC 1213  
     definition [1-14](#)  
 RJ-45 twisted pair connector [1-6](#)  
 RRP's  
     AC module [5-24](#)  
     backplane [5-35](#)  
     CTP card [5-6](#)  
     ESD information [5-3](#)  
     ESD precautions [5-2](#)  
     fan module [5-27](#)  
     power supply [5-20](#)  
     Power/System Error LED assembly [5-30](#)  
     procedural notes [5-2](#)  
     SBAR assembly [5-31](#)  
     SFP optical transceiver [5-15](#)  
     UPM card [5-10](#)  
     UPM filler panel [5-19](#)  
     XFP optical transceiver [5-15](#)  
     XPM card [5-10](#)  
     XPM filler panel [5-19](#)

- RS-232
  - maintenance port 1-6
- RSCN
  - suppress zoning messages 2-90
- S**
- SA OS/390 2-47
- safety
  - caution statements -xxviii, F-1
  - danger statements -xxviii, F-1
  - ESD
    - FRUs, removing and replacing 5-2
    - information 5-3
    - repair procedures 4-2
  - ESD grounding cable with wrist strap 1-17
  - ESD precautions -xxix
  - fiber-optic protective plug 1-16
  - general precautions -xxix
  - laser compliance -xxvi
  - multi-lingual notices F-1
- safety notices, multi-lingual F-1
- SAN management application
  - default password E-7
  - default user name E-7
- SANpilot
  - disable at management server 2-73
  - enable at management server 2-73
  - ethernet link, MAP 3-56
  - fault isolation 3-9
- SANpilot interface
  - See SANpilot
- SBAR assembly
  - description 1-11
  - event codes B-61
  - frame transmission 1-6
  - LEDs 1-12
  - MAP 3-74
  - removing and replacing 5-31
- segmentation
  - MAP 3-104
- segmented e\_port
  - description 2-89
- serial numbers, FRUs, hardware log 4-8
- service contract -xxvii
- serviceability features, director 1-12
- session log 4-5
- setting
  - date and time 2-50
  - offline state 4-44
  - online state 4-44
- SFP optical transceiver 1-9
  - MAP 3-82
  - removing and replacing 5-15
- shipping environment, director C-2
- simple mail transfer protocol 2-73
- site plan 2-8
- small form factor pluggable optical transceiver
  - See SFP optical transceiver
- SMTP server address 2-73
- SNMP
  - configure at SANpilot 2-95
  - general description 1-18
  - trap messages, configure recipients 2-66
  - trap messages, maximum recipients 1-14
- software
  - download EFC Manager application from file center 4-82
  - installing 4-82
  - upgrading 4-82
- spare parts
  - See FRUs
- specifications, director C-1
- specifications, management server D-2
- SSP subsystem 1-6
- statistical information, performance view 4-16
- statistics
  - clear for port 4-24
  - counter 4-25
  - wraps 4-25
- storage environment, director C-2
- subnet mask
  - change director value 2-93
  - default 2-1, 3-2, 4-2, 5-1
- suppress zoning RSCN 2-90
- swapping ports, procedure 4-38
- switch
  - principal, configure 2-56
  - principal, configuring 3-115
  - priority value, configure 2-56
  - priority value, configuring 3-115
  - priority, default 2-56, 3-115
- switch binding
  - configure 2-101

- description 2-101
- disable 2-60
- enable 2-60
- online state requirements 2-59
- switch binding membership list
  - configuring 2-104
  - overview 2-102
- switch priority 2-92
- synchronizing date and time 2-51
- system error LED 1-5
- system events
  - event codes B-3
- system services processor 1-6

**T**

TCP/IP MIB-II

- definition 1-14

technical support

- file center registration 2-120

Telnet access

- disable at management server 2-73
- enable at management server 2-73

temperature

- operating environment C-2
- shipping and storage environment C-2

thermal events

- event codes B-67

threshold alert

- configure 2-67
- port properties dialog box 4-22
- reasons for 4-22

TightVNC

- default password 2-26, 2-80, 4-88, E-5

Tivoli NetView 2-46

tools

- AC module 5-24
- backplane 5-35
- CTP card 5-6
- fan module 5-27
- power supply 5-20
- Power/System Error LED assembly 5-30
- SBAR assembly 5-31
- SFP optical transceiver 5-15
- supplied by service personnel 1-17
- supplied with director 1-15
- UPM card 5-10

- UPM filler panel 5-19
- XFP optical transceiver 5-15
- XPM card 5-10
- XPM filler panel 5-19
- torque tool 1-15
  - caution 1-15
- trademarks -xxvi
- transceivers, compliance -xxvi
- trap message recipients 2-66
- trap messages, maximum recipients 1-14

## U

- unblock ports
  - from SANpilot 4-50
- unblocking
  - port 4-47
  - UPM card 4-48
  - XPM card 4-48
- Unpack 2-12
- upgrading software 4-82
- UPM card
  - blocking 4-47
  - description 1-7
  - event codes B-48
  - LEDs 1-7, 4-13
  - loopback test, performing 4-30
  - MAP 3-82
  - ports, blocking or unblocking 4-46
  - removing and replacing 5-10
  - unblocking 4-48
- UPM filler panel, removing and replacing 5-19
- user name
  - default EFC Manager 4-89
  - default EFC manager 2-80
  - default SAN management application E-7
  - default SANpilot 2-83
  - default Windows 2000 2-27, 2-80, 4-89, E-6

## V

- velocity, angular, of fans 1-11
- verifying
  - director, management server communication 2-43
  - installation requirements 2-8
- Veritas SANPoint Control 2-46
- versions

FC fabric element MIB [1-14](#)

firmware

adding [4-56](#)

determining [4-56](#)

downloading [4-63](#)

managing [4-55](#)

NetView [2-46](#)

SA OS/390 [2-47](#)

SANPoint [2-46](#)

Windows operating systems [1-18](#)

views

performance [4-16](#)

port list [4-15](#)

voltage

AC power connectors [1-11](#)

backplane [1-12](#)

director [C-1](#)

power supply [1-11](#)

## W

warranty [-xxvii](#)

weight, director [C-1](#)

wet-bulb temperature

operating environment [C-2](#)

shipping and storage environment [C-2](#)

Windows 2000

configure users [2-30](#)

default password [2-27](#), [2-80](#), [4-89](#), [E-6](#)

default user name [2-27](#), [2-80](#), [4-89](#), [E-6](#)

Windows operating systems, versions [1-18](#)

world-wide name

See WWN

wraps, definition [4-25](#)

WWN

port properties dialog box [4-21](#)

## X

XFP optical transceiver [1-9](#)

MAP [3-82](#)

removing and replacing [5-15](#)

XPM card

blocking [4-47](#)

description [1-8](#)

event codes [B-48](#)

LEDs [1-8](#), [4-13](#)

loopback test, performing [4-30](#)

MAP [3-82](#)

ports, blocking or unblocking [4-46](#)

removing and replacing [5-10](#)

unblocking [4-48](#)

XPM filler panel, removing and replacing [5-19](#)

## Z

zone sets

configure at SANpilot [2-117](#)

description [2-114](#)

zones

add or delete members [2-116](#)

configure at SANpilot [2-114](#)

description [2-113](#)